Avira AntiVir Personal – Free Antivirus

Manuale utente

AVIRA®

Marchio registrato e copyright

Marchio registrato

AntiVir è un marchio registrato di Avira GmbH.
Windows è un marchio registrato di Microsoft Corporation negli Stati Uniti e in altri paesi.
Tutti gli altri marchi o nomi di prodotti sono marchi registrati del legittimo proprietario.
I marchi protetti non sono contrassegnati come tali in questo manuale. Ciò tuttavia non significa che possano essere liberamente utilizzati.

Note sul Copyright

Per Avira AntiVir Personal è stato utilizzato codice di terzi. Ringraziamo i possessori di copyright per aver messo a disposizione il proprio codice. Informazioni dettagliate sul copyright sono disponibili nella Guida in linea di Avira AntiVir Personal in Third Party Licenses.

Sommario

1 Introduzione 1

2 Simboli ed evidenziazioni 2

3 Informazioni sul prodotto 3

3.1 Prestazioni 3
3.2 Requisiti di sistema 4
3.3 Licenza e aggiornamento 5

4 Installazione e disinstallazione 6

4.1 Installazione 6
4.2 Modifiche all'installazione 10
4.3 Moduli di installazione 10
4.4 Disinstallazione 11

5 AntiVir Personal in sintesi 12

5.1 Interfaccia utente e funzionamento 12
5.1.1 Control Center 12
5.1.2 Configurazione 14
5.1.3 Icona Tray 17
5.2 Come procedere 17
5.2.1 Aggiornare automaticamente Avira AntiVir Personal 17
5.2.2 Avvio di un aggiornamento manuale 19
5.2.3 Scansione diretta: Eseguire il controllo di virus e malware con un profilo di ricerca 19
5.2.4 Scansione diretta: Ricerca di virus e malware con Drag&Drop 20
5.2.5 Scansione diretta: Ricerca di virus e malware con il menu contestuale 20
5.2.6 Scansione diretta: Cercare automaticamente virus e malware 21
5.2.7 Scansione diretta: Effettuare una scansione mirata per rootkit attivi 22
5.2.8 Reagire a virus e malware riscontrati 22
5.2.9 Quarantena: Trattare file (*.qua) in quarantena 24
5.2.10 Quarantena: Ripristinare file in quarantena 25
5.2.11 Quarantena: Spostare i file sospetti in quarantena 26
5.2.12 Profilo di ricerca: Inserire o eliminare un tipo di file in un profilo di ricerca 27
5.2.13 Profilo di ricerca: Creare un collegamento sul desktop per il profilo di ricerca 27
5.2.14 Eventi: filtrare eventi 27

6 Scanner 30

7 Aggiornamenti 31

8 FAQ, suggerimenti 32

8.1 Assistenza in caso di problemi 32
8.2 Shortcut 33
8.2.1 Nelle finestre di dialogo 34
8.2.2 Nella Guida in linea 34
8.2.3 In Control Center 35
8.3 Centro sicurezza di Windows 36
8.3.1 Generale 36
8.3.2 Il Centro sicurezza di Windows e Avira AntiVir Personal 36

9 Virus e altro 39

9.1 Categorie estese delle minacce 39
9.2 Virus e altri malware 41

10 Info e Service 45

10.1 Indirizzi di contatto 45
10.2 Supporto tecnico 45
10.3 File sospetto 45
10.4 Comunicare un falso allarme 46

11 Riferimento: Opzioni di configurazione 47

11.1 Sistema di scansione 47
11.1.1 Scansione 47
11.1.1.1. Azione in caso di rilevamento 50
11.1.1.2. Eccezioni 52
11.1.1.3. Euristica 53
11.1.2 Report 54
11.2 Guard 54
11.2.1 Scansione 55
11.2.1.1. Azione in caso di rilevamento 56
11.2.1.2. Eccezioni 57
11.2.1.3. Euristica 60
11.2.2 Report 60
11.3 Aggiornamento 61
11.3.1 Aggiornamento prodotto 62
11.3.2 Impostazioni riavvio 63
11.3.3 Server web 63
11.3.3.1. Proxy 64
11.4 Generale 65
11.4.1 Configurazione :: Generale 65
11.4.2 Sicurezza 65
11.4.3 WMI 66
11.4.4 Directory 67
11.4.5 Eventi 67
11.4.6 Limita i report 68
11.4.7 Avvisi acustici 68
11.4.8 Avvisi 69

1 Introduzione

Avira AntiVir Personal di Avira GmbH protegge efficacemente il computer da virus, malware, spyware, programmi indesiderati e altri pericoli. In questo manuale si parlerà riduttivamente di virus e malware.

La guida descrive l'installazione e il funzionamento del programma.

Sul nostro sito Internet http://www.avira.it/free-av è possibile scaricare il manuale relativo a Avira AntiVir Personal in PDF, aggiornare Avira AntiVir Personal o informarsi sulla versione a pagamento Avira AntiVir Premium .

Inoltre sul nostro sito Internet sono disponibili informazioni come ad esempio numeri telefonici del Supporto tecnico o le nostre newsletter a cui è possibile abbonarsi.

Il Suo team di Avira GmbH

2 Simboli ed evidenziazioni

Si utilizzano i seguenti simboli:

Simbolo/Definizione	Spiegazione
✓	Esiste un requisito che deve essere soddisfatto prima che sia eseguita un'operazione.
▸	Prima di un'operazione che deve essere eseguita dall'utente.
→	Prima di un evento scaturito dall'operazione precedente.
Attenzione	Prima di un avviso di pericolo di una significativa perdita di dati.
Nota	Prima di un messaggio con informazioni particolarmente importanti o prima di un suggerimento che agevola la comprensione e l'uso di Avira AntiVir Personal.

Si utilizzano le seguenti evidenziazioni:

Evidenziazione	Spiegazione
Corsivo	Nome del file o percorso.
	Elementi dell'interfaccia del software che vengono visualizzati (ad esempio titolo della finestra, sezione o campo di opzione).
Grassetto	Elementi dell'interfaccia software, su cui è possibile fare clic (ad es. voci di menu, rubriche o pulsanti).

3 Informazioni sul prodotto

In questo capitolo è possibile consultare tutte le informazioni rilevanti per l'acquisto o l'utilizzo di Avira AntiVir Personal:

- vedere capitolo: Prestazioni
- vedere capitolo: Requisiti di sistema
- vedere capitolo: Licenza

Avira AntiVir Personal è uno strumento utile e completo per proteggere efficacemente il computer da virus, malware, programmi indesiderati e altri pericoli.

▶ Prestare attenzione ai seguenti suggerimenti:

Nota
La perdita di dati importanti ha spesso conseguenze drammatiche. Nemmeno il miglior programma antivirus può offrire una protezione al 100% contro la perdita di dati. Si consiglia di eseguire regolarmente copie di sicurezza (backup) dei dati.

Nota
Un programma in grado di proteggere il computer da virus, malware, programmi indesiderati e altri pericoli può essere affidabile ed efficace solo se aggiornato regolarmente. Si consiglia di garantire l'aggiornamento di Avira AntiVir Personal con gli aggiornamenti automatici. Configurare il programma in modo adeguato.

3.1 Prestazioni

Avira AntiVir Personal offre le seguenti funzioni:

- Control Center per il monitoraggio, l'amministrazione e la gestione dell'intero programma
- Configurazione centrale con configurazione semplice in modalità esperto oppure standard e dotata di guida in linea sensibile al contesto
- Scanner (On-Demand Scan) con scansione di tutti i tipi noti di virus e malware gestita dal profilo e configurabile
- Integrazione nella funzionalità di controllo di Windows Vista (Controllo dell'account utente) per poter eseguire operazioni per le quali sono necessari i diritti di amministratore
- Guard (On-Access Scan) per il costante monitoraggio di tutti gli accessi ai file
- Gestione integrata della quarantena per l'isolamento e il trattamento di file sospetti
- Protezione rootkit per il rilevamento di malware installatisi occultamente nel sistema del computer (i cosiddetti rootkit)
  (non disponibile in Windows XP 64 Bit)
- Accesso diretto in Internet a informazioni dettagliate su virus rilevati e malware
- Aggiornamento semplice e rapido del programma, delle definizioni dei virus (VDF) e del motore di ricerca tramite aggiornamento di file singolo e aggiornamento VDF incrementale mediante un server Web su Internet
- Scheduler integrato per la pianificazione di operazioni singole o ricorrenti come aggiornamenti o scansioni

- Identificazione estremamente precisa di virus e malware per mezzo di tecnologie di ricerca (motore di ricerca) che includono la procedura di ricerca euristica
- Identificazione di tutti i tipi di archivio convenzionali, inclusa l'identificazione di archivi nascosti e Smart-Extension
- Elevata performance grazie alla capacità multi threading (scansione contemporanea di molti file ad alta velocità)

3.2 Requisiti di sistema

Perché Avira AntiVir Personal funzioni correttamente, il sistema deve soddisfare i requisiti seguenti:

- Computer a partire dal Pentium, minimo 266 MHz
- Sistema operativo
- Windows 2000, SP4 e rollup di aggiornamento 1 o
- Windows XP, SP2 (32 o 64 Bit) o
- Windows Vista (32 o 64 Bit, SP 1 consigliato)
- Windows 7 (32 o 64 Bit)
- Min. 150 MB di memoria libera sull'hard disk (se si utilizza la quarantena e la memoria temporanea maggiore quantità di memoria)
- Min. 256 MB di memoria di lavoro in Windows 2000/XP
- Min. 1024 MB di memoria di lavoro in Windows Vista, Windows 7
- Per l'installazione di Avira AntiVir Personal: diritti di amministratore
- Per tutte le installazioni: Windows Internet Explorer 6.0 o superiore
- Eventuale disponibilità di connessione a Internet (vedasi Installazione)

Note per l'utente di Windows Vista

In Windows 2000 e Windows XP molti utenti lavorano con i diritti di amministratore. Dal punto di vista della sicurezza tuttavia questo non è auspicabile, perché in questo modo sarà facile anche per virus o programmi indesiderati annidarsi nel computer.

Per questo motivo Microsoft ha aggiunto in Windows Vista il "Controllo utente" (User Account Control). Esso offre una maggiore protezione per gli utenti che sono registrati come amministratori: Pertanto un amministratore dispone, in Windows Vista, dapprima dei soli privilegi di normale utente. Azioni, per le quali è necessario possedere i diritti di amministratore, sono evidenziate da Windows Vista chiaramente con un punto esclamativo. Inoltre l'utente deve esplicitamente confermare l’azione desiderata. Solo dopo aver ricevuto questa conferma, aumentano i privilegi, e il sistema operativo esegue la funzione amministrativa corrispondente.

Avira AntiVir Personal necessita dei diritti di amministratore per eseguire alcune azioni in Windows Vista. Queste azioni sono contrassegnate con il seguente carattere: . Se questo carattere appare inoltre su un pulsante, significa che per l'esecuzione di tale azione sono necessari i diritti di amministratore. Se il suo account attuale non gode dei diritti di amministratore, in Windows Vista appare la finestra di dialogo Controllo Utente per l’introduzione della password dell’amministratore. Se non dispone della password dell’amministratore, non può eseguire tale azione.

3.3 Licenza e aggiornamento

Per poter utilizzare Avira AntiVir Personal è necessario possedere una licenza. In questo modo si prende visione delle condizioni di licenza di Avira AntiVir Personal.

La licenza viene assegnata sotto forma di una chiave di attivazione. La chiave di attivazione è un codice alfanumerico che l'utente riceve all'acquisto di Avira AntiVir Personal. La chiave di attivazione comprende i dati esatti della licenza, ossia quali sono i programmi dotati di licenza e per quale periodo.

Nel caso AntiVir Personal sia stato acquistato su Internet, l'utente riceverà la chiave di attivazione per email, altrimenti è riportata sulla confezione del prodotto.

Per attivare la licenza del programma, è necessario immettere tale chiave durante l'attivazione di Avira AntiVir Personal. L'attivazione del prodotto può avvenire durante l'installazione. Tuttavia, è possibile attivare Avira AntiVir Personal anche in seguito nel Sistema di gestione delle licenze in Guida in linea::Sistema di gestione delle licenze.

In Avira AntiVir Personal è già contenuta una chiave di attivazione valida. In questo modo si evita la procedura di attivazione del prodotto.

Nel Sistema di gestione delle licenze è possibile avviare un aggiornamento a un prodotto della famiglia AntiVir Desktop: In questo modo non è necessario disinstallare il vecchio prodotto manualmente e installare manualmente il nuovo. Tramite l'aggiornamento dal Sistema di gestione delle licenze immettere nell'apposito campo la chiave di attivazione del prodotto di cui si desidera effettuare l'aggiornamento. Il nuovo prodotto viene installato automaticamente.

Tramite il Sistema di gestione delle licenze è possibile effettuare l'aggiornamento automatico dei seguenti prodotti:

- Aggiornamento di Avira AntiVir Personal ad Avira AntiVir Premium
- Aggiornamento da Avira AntiVir Personal a Avira Premium Security Suite
- Aggiornamento da Avira AntiVir Premium a Avira Premium Security Suite

4 Installazione e disinstallazione

In questo capitolo si ottengono informazioni relative all'installazione e la disinstallazione di Avira AntiVir Personal:

- vedere capitolo Installazione: requisiti, modalità di installazione, esecuzione dell'installazione
- vedere capitolo Moduli di installazione
- vedere capitolo Modifica dell'installazione
- vedere capitolo Disinstallazione: Eesegui disinstallazione

4.1 Installazione

Prima dell'installazione di Avira AntiVir Personal verificare che il computer risponda ai requisiti minimi del sistema. Se il computer soddisfa i requisiti minimi è possibile installare Avira AntiVir Personal.

Nota
Da Windows XP in poi Avira AntiVir Personal crea un punto di ripristino prima dell'installazione di Avira AntiVir Personal. Ciò permette di rimuovere in maniera sicura Avira AntiVir Personal in caso di installazione non riuscita. Si prega di prestare attenzione al fatto che l'opzione **Disattiva ripristino configurazione di sistema** in: "Start | Impostazioni | Pannello di controllo | Sistema | Scheda Ripristino configurazione di sistema" non deve essere selezionata.
Se si desidera ripristinate il computer a uno stato precedente è possibile farlo con la funzione "Start | Programmi | Accessori | Utilità di sistema | Ripristino configurazione di sistema". Il punto di ripristino creato da Avira AntiVir Personal è riconoscibile alla voce AntiVir Personal.

Tipi di installazione

Durante l'installazione mediante l'assistente di installazione è possibile selezionare un tipo di setup:

Express

- Non verranno installati tutti i componenti del programma disponibili. I seguenti componenti software non vengono installati:

AntiVir ProActiv

AntiVir FireWall

- I file del programma vengono installati in una directory standard predefinita in `C:\Programmi`.
- AntiVir Personal viene installato unitamente alle impostazioni di default. È possibile effettuare impostazioni predefinite nell'assistente di configurazione.

Personalizzata

- Con l'installazione personalizzata è possibile selezionare singole componenti del programma (vedere capitolo Installazione e disinstallazione::Moduli di installazione).
- Si può scegliere una cartella di destinazione per i file di programma da installare.
- È possibile disattivare la creazione di un'icona sul desktop e di un gruppo di programmi nel menu di avvio.
- Nella configurazione guidata è possibile effettuare impostazioni predefinite di AntiVir Personal e lanciare una breve scansione del sistema, che viene eseguita automaticamente dopo l'installazione.

Prima dell'avvio della procedura di installazione

- Chiudere il programma email. Si consiglia inoltre di chiudere tutte le applicazioni in uso.
- Assicurarsi che non siano installate altre protezioni contro virus. Le funzioni automatiche di protezione di diverse applicazioni antivirus potrebbero entrare in conflitto.
- Stabilire una connessione Internet. La connessione a Internet è necessaria per eseguire i seguenti passaggi dell'installazione:
- Scaricare i file attuali di programma e del motore di ricerca, nonché i file di definizione dei virus aggiornati mediante il programma di installazione (per installazione basata su Internet)
- Registrarsi come utente di Avira AntiVir Personal
- Aggiornare, se necessario, AntiVir Personal a installazione conclusa
- Tenere a portata di mano la chiave di licenza per AntiVir Personal se si desidera attivare AntiVir Personal.

Nota
Installazione basata su Internet:
per eseguire un'installazione basata su Internet di Avira AntiVir Personal, Avira GmbH mette a disposizione un programma di installazione che carica i file di programma attuali prima di eseguire l'installazione dai server Web di Avira GmbH. Tale procedura garantisce l'installazione di AntiVir Personal con un file di definizione dei virus aggiornato.
Installazione con un pacchetto di installazione:
il pacchetto di installazione contiene sia il programma di installazione sia tutti i file di programma necessari. Tuttavia nell'installazione con un pacchetto di installazione non è possibile effettuare la selezione della lingua per AntiVir Personal. Al termine dell'installazione si consiglia di eseguire un aggiornamento del file di definizione dei virus.

Nota
Per la registrazione Avira AntiVir Personal comunica con i server di Avira GmbH tramite il protocollo HTTP e la porta 80 (comunicazione Web) nonché tramite il protocollo di codifica SSL e la porta 443. Se si utilizza un firewall, assicurarsi che la connessione necessaria e i dati in entrata e in uscita non vengano bloccati dal firewall.

Eseguire l'installazione

Il programma di installazione funziona in modalità di dialogo. Ogni finestra contiene una determinata selezione di pulsanti per la gestione del processo di installazione.

I pulsanti principali hanno le seguenti funzioni:

- **OK:** per confermare l'azione.
- **Annulla:** per annullare l'azione.
- **Continua:** per passare alla fase successiva.
- **Indietro:** per passare alla fase precedente.

Installare AntiVir Personal nel modo seguente:

▶ Avviare il programma di installazione facendo doppio clic sul file di installazione scaricato da Internet o inserire il CD del programma.

Installazione basata su Internet

→ Appare la finestra di dialogo *Benvenuti...*.

▶ Fare clic su **Avanti** per continuare l'installazione.

→ Appare la finestra di dialogo *Seleziona lingua*.

▶ Selezionare la lingua con cui si desidera installare AntiVir Personal, e confermare con **Avanti**.

→ Appare la finestra di dialogo *Download*. Tutti i file necessari per l'installazione vengono scaricati dai server Web di Avira GmbH. Al termine del download la finestra *Download* si chiude.

Installazione con un pacchetto di installazione

→ L'assistente di installazione si apre con la finestra di dialogo *Avira AntiVir Personal*.

▶ Fare clic su *Accetta* per avviare l'installazione.

→ Il file di installazione viene decompresso. La routine di installazione viene avviata.

→ Appare la finestra di dialogo *Benvenuti...*.

▶ Fare clic su **Avanti**.

Prosecuzione dell'installazione basata su Internet o dell'installazione con un pacchetto di installazione

→ Appare ora la finestra di dialogo con l'accordo di licenza.

▶ Confermare l'accettazione della licenza e fare clic su **Avanti**.

→ Appare la finestra di dialogo *Uso privato*.

▶ Confermare che si utilizza AntiVir Personal esclusivamente per scopi privati e non commerciali e fare clic su **Avanti**.

→ Appare la finestra di dialogo *Crea numero di serie*.

▶ Confermare, se richiesto, che si è generato un numero di serie casuale che verrà riportato durante l'aggiornamento e fare clic su **Avanti**.

→ Appare la finestra di dialogo *Seleziona il tipo di installazione*.

▶ Decidere se si desidera eseguire un'installazione Express o personalizzata.

▶ Attivare l'opzione **Express** o **Personalizzata** e confermare con **Avanti**.

Installazione personalizzata

→ Appare la finestra *Selezionare directory di destinazione*.

▶ Confermare la directory di destinazione con **Avanti**.

- OPPURE -

Selezionare con **Sfoglia** un'altra directory di destinazione e confermare con **Avanti**.

→ Appare la finestra *Installare componenti*:

▶ Attivare o disattivare i componenti desiderati e confermare con **Avanti**.

→ Nelle seguenti finestre di dialogo è possibile stabilire se creare o meno un collegamento sul desktop e/o un gruppo di programmi sul menu.

▶ Fare clic su **Avanti**.

Prosecuzione: installazione Express e personalizzata

→ Si apre l'assistente per l'installazione della licenza.

Nell'assistente per l'installazione della licenza è possibile registrarsi come cliente di AntiVir Personal e abbonarsi alla newsletter di Avira GmbH. A tal fine è necessario immettere i propri dati personali.

▶ Inserire eventualmente i propri dati e confermarli con **Avanti**.

→ Durante la registrazione, nella seguente finestra di dialogo viene visualizzato il risultato dell'attivazione.

→ Fare clic su **Avanti**.

→ I componenti del programma vengono installati. L'avanzamento dell'installazione viene visualizzato nella finestra di dialogo.

→ Nella finestra di dialogo seguente è possibile decidere se, una volta terminata l'installazione, il file readme deve essere aperto e il sistema deve essere riavviato.

▶ Accettare se si desidera e fare clic su *Fine* per terminare l'installazione.

→ L'assistente di installazione si chiude.

Prosecuzione: Installazione personalizzata
Assistente di configurazione

→ Nell'installazione personalizzata nel passaggio successivo si apre l'assistente di configurazione. Nell'assistente di configurazione è possibile effettuare importanti impostazioni predefinite per AntiVir Personal.

▶ Fare clic su **Avanti** nella finestra di benvenuto dell'assistente di configurazione per iniziare la configurazione di AntiVir Personal.

→ Nella finestra di dialogo *Configura AHeAD* è possibile selezionare un livello di riconoscimento per la tecnologia AHeAD. Il livello di riconoscimento selezionato viene registrato per l'impostazione della tecnologia AHeAD di Scanner (scansione diretta) e di Guard (scansione in tempo reale).

▶ Selezionare un livello di riconoscimento e proseguire la configurazione con **Avanti**.

→ Nella finestra di dialogo seguente *Seleziona categorie estese delle minacce* è possibile adattare le funzioni di protezione di AntiVir Personal con la selezione delle categorie delle minacce.

▶ Attivare eventualmente ulteriori categorie delle minacce e proseguire la configurazione con *Avanti*.

→ Nel caso in cui si sia selezionato il modulo di installazione AntiVir Guard, appare la finestra di dialogo *Modalità di avvio Guard*. È ora possibile stabilire il momento in cui avviare Guard. Nella modalità di avvio indicata Guard viene avviato a ogni riavvio del computer.

Nota
La modalità di avvio indicata di Guard viene memorizzata nel registro e non può essere modificata mediante la configurazione.

▶ Attivare l'opzione desiderata e proseguire la configurazione con *Avanti*.

→ Nella finestra di dialogo seguente *Scansione del sistema* è possibile attivare o disattivare l'esecuzione di una scansione rapida del sistema. La scansione rapida del sistema viene eseguita al termine della configurazione e prima di riavviare il computer, e verifica la presenza di virus e malware nei programmi avviati e nei file di sistema più importanti.

▶ Attivare o disattivare l'opzione *Scansione rapida del sistema* e proseguire la configurazione con *Avanti*.

→ Nella finestra di dialogo seguente è possibile terminare la configurazione con *Fine*.

▶ Fare clic su *Fine* per terminare la configurazione.

→ Le impostazioni indicate e selezionate vengono registrate.

→ Se è attivata l'opzione *Scansione rapida del sistema* si apre la finestra Luke Filewalker. Scanner esegue una scansione rapida del sistema.

Prosecuzione: Installazione Express e personalizzata

→ Se nell'ultima installazione mediante assistente è stata selezionata l'opzione **Riavvia computer**, il calcolatore si riavvia.

→ Una volta terminato il riavvio del computer, se nell'installazione mediante assistente è stata selezionata l'opzione **Visualizza ReadMe**, viene visualizzato il file readme di AntiVir Personal.

Se l'installazione è avvenuta con successo si consiglia di verificare lo stato di aggiornamento di AntiVir Personal in *Panoramica :: Stato* nel Control Center.

▶ Se necessario eseguire un aggiornamento di AntiVir Personal per aggiornare il file di definizione dei virus.

▶ Infine eseguire una scansione completa del sistema.

4.2 Modifiche all'installazione

Si ha la possibilità di aggiungere o rimuovere singole componenti del programma all'attuale installazione di Avira AntiVir Personal (vedere capitolo Installazione e disinstallazione::Moduli di installazione)

Se si desidera aggiungere o eliminare componenti del programma dell'installazione corrente di Avira AntiVir Personal è possibile utilizzare l'opzione **Installazione applicazioni**, **Cambia/Rimuovi programmi** all'interno del **Pannello di controllo di Windows**.

Selezionare Avira AntiVir Personal e fare clic su **Cambia**. Nella finestra di dialogo di benvenuto di Avira AntiVir Personal selezionare l'opzione **Modifica**. Si è così inseriti nella modifica dell'installazione.

4.3 Moduli di installazione

Nel caso di un'installazione personalizzata o di una modifica di un'installazione è possibile selezionare, aggiungere o eliminare i seguenti moduli:

- **AntiVir Personal**
  Questo modulo contiene tutte le componenti necessarie per l'installazione corretta di Avira AntiVir Personal.
- **AntiVir Guard**
  AntiVir Guard è in esecuzione in background. Monitora e ripara i file, quando possibile, durante operazioni come apertura, scrittura e copia in tempo reale (On-Access = all'accesso). Se un utente esegue un'operazione (caricamento, esecuzione, copia di un file) Avira AntiVir Personal scansiona automaticamente il file. Durante l'operazione di rinomina del file AntiVir Guard non esegue alcuna scansione.
- ***Protezione rootkit di AntiVir***
  La Protezione rootkit di AntiVir controlla se sul computer sono già installati software che dopo l'intrusione nel computer non si riesce a rilevare con i metodi convenzionali del riconoscimento di malware.
- **Shell Extension**
  Le estensioni shell di Avira AntiVir Personal creano nel menu contestuale di Esplora risorse di Windows (tasto destro del mouse) la voce Controlla i file selezionati con AntiVir. Con questa voce è possibile scansionare direttamente singoli file o directory.

4.4 Disinstallazione

Se si desidera eliminare Avira AntiVir Personal dal proprio computer, è possibile utilizzare l'opzione **Cambia/Rimuovi programmi** di **Installazione applicazioni** nel Pannello di controllo di Windows.

Si può disinstallare Avira AntiVir Personal (descritto ad esempio per Windows XP e Windows Vista) nel seguente modo:

- ▶ Aprire nel menu **Start** di Windows il **Pannello di controllo**.
- ▶ Fare doppio clic su **Programmi**(Windows XP: **Installazione applicazioni**).
- ▶ Selezionare **Avira AntiVir Personal** e fare clic su **Rimuovi**.
- → Verrà chiesto all'utente se desidera davvero eliminare il programma.
- ▶ Confermare con **Sì**.
- → Tutte le componenti del programma vengono eliminate.
- ▶ Fare clic su **Fine** per terminare la disinstallazione.
- → Appare una finestra di dialogo con il suggerimento di riavviare il computer.
- ▶ Confermare con **Sì**.

→ Avira AntiVir Personal è disinstallato, se stabilito il computer verrà riavviato e tutte le directory, i file e gli inserimenti del registro verranno eliminati da Avira AntiVir Personal.

5 AntiVir Personal in sintesi

In questo capitolo è possibile consultare una panoramica delle funzionalità e del funzionamento di AntiVir Personal.

- vedere capitolo Interfaccia e funzionamento
- vedere capitolo Come procedere

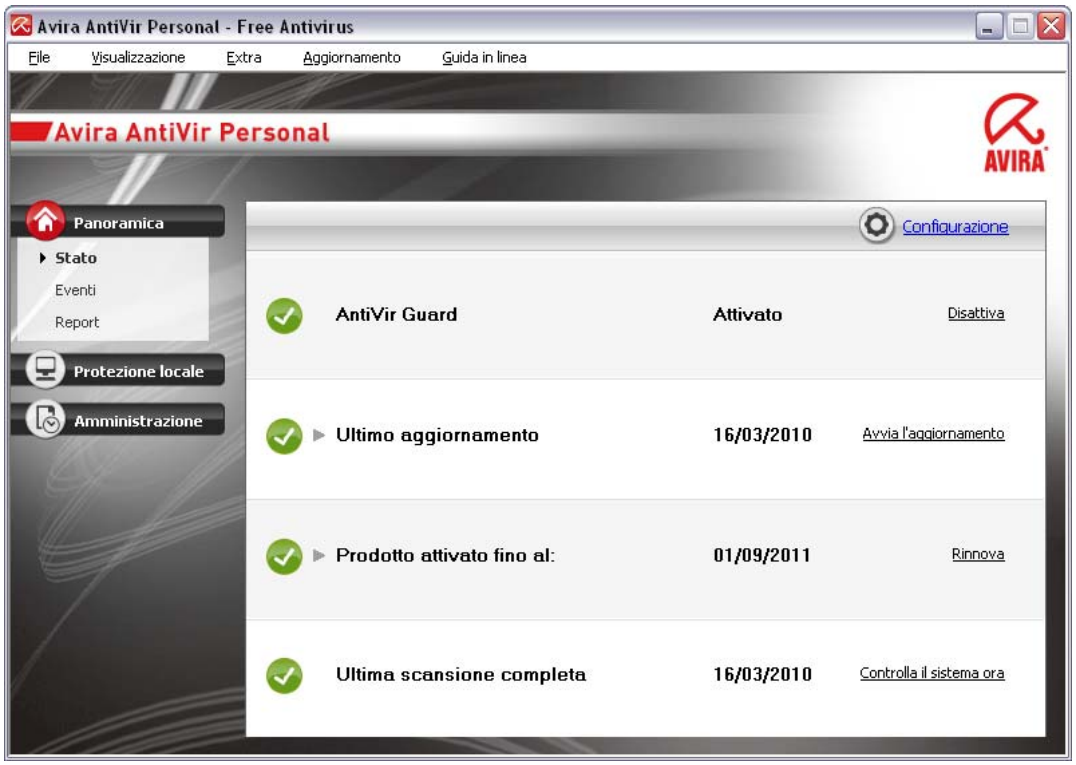
5.1 Interfaccia utente e funzionamento

É possibile usare AntiVir Personal mediante tre elementi dell'interfaccia del programma:

- Control Center: Monitoraggio e gestione di AntiVir Personal
- Configurazione: Configurazione di AntiVir Personal
- Icona Tray della barra delle applicazioni: Apertura di Control Center e altre funzioni

5.1.1 Control Center

Il Control Center serve per il monitoraggio dello stato di protezione del computer e per la gestione e il funzionamento delle componenti di protezione e delle funzioni di AntiVir Personal.



La finestra di Control Center è divisa in tre sezioni: l'**elenco menu**, la **barra di navigazione** e la finestra per i dettagli **Visualizza**:

- **Elenco menu:** nei menu di Control Center è possibile richiamare funzioni generali del programma e informazioni su AntiVir Personal.

- **Sezione di navigazione:** nella sezione di navigazione è possibile passare in modo semplice da una rubrica all'altra di Control Center. Le singole rubriche contengono informazioni e funzioni delle componenti del programma AntiVir Personal e sono presenti sulla barra di navigazione in base alle sezioni dei task. Esempio: sezione dei task *Panoramica* - Rubrica **Stato**.
- **Visualizza:** in questa finestra viene visualizzata la categoria che è stata selezionata nella sezione di navigazione. In base alla rubrica nella barra superiore della finestra dei dettagli sono presenti pulsanti per l'esecuzione di funzioni o azioni. Nelle singole rubriche vengono visualizzati dati o oggetti presenti negli elenchi. É possibile ordinare le liste facendo clic sul campo in base al quale si desidera ordinare le stesse.

Avvio e chiusura di Control Center

Per avviare Control Center è possibile scegliere tra le seguenti modalità:

- fare doppio clic sull'icona del programma sul desktop
- mediante la voce del programma di AntiVir Personal nel menu Start | Programmi.
- mediante la Icona Tray di Avira AntiVir Personal.

Si può chiudere Control Center mediante il comando **Chiudi** nel menu **File** o facendo clic sulla x nella finestra di Control Center.

Utilizzo di Control Center

Come navigare in Control Center

▶ Selezionare una sezione dei task nella barra di navigazione.

→ La sezione dei task si apre e appaiono diverse rubriche. La prima rubrica della sezione dei task viene selezionata e visualizzata.

▶ Fare clic su un'altra categoria per visualizzarla nella finestra dei dettagli.

- OPPURE -

▶ Selezionare una categoria mediante il menu *Visualizza*.

Nota
Attivare la navigazione da tastiera nell'elenco menu con l'ausilio del tasto [Alt]. Se la navigazione con tastiera è attivata, è possibile spostarsi all'interno dei menu con i tasti freccia. Con il tasto Invio si attiva la voce di menu selezionata in quel momento.
Per aprire, chiudere o navigare nei menu di Control Center è possibile utilizzare anche le combinazioni di tasti: tasto [Alt] + lettera sottolineata nel menu o nel comando. Tenere premuto il tasto [Alt] se si desidera richiamare dal menu un comando o un sottomenu.

Come elaborare dati o oggetti che vengono visualizzati nella finestra dei dettagli:

▶ Evidenziare i dati o gli oggetti che si desidera elaborare.

Per evidenziare più elementi, tenere premuto il tasto Ctrl o il tasto Shift (selezione di elementi consecutivi) durante la selezione degli elementi.

▶ Fare clic sui pulsanti desiderati nella barra superiore della finestra dei dettagli per elaborare l'oggetto.

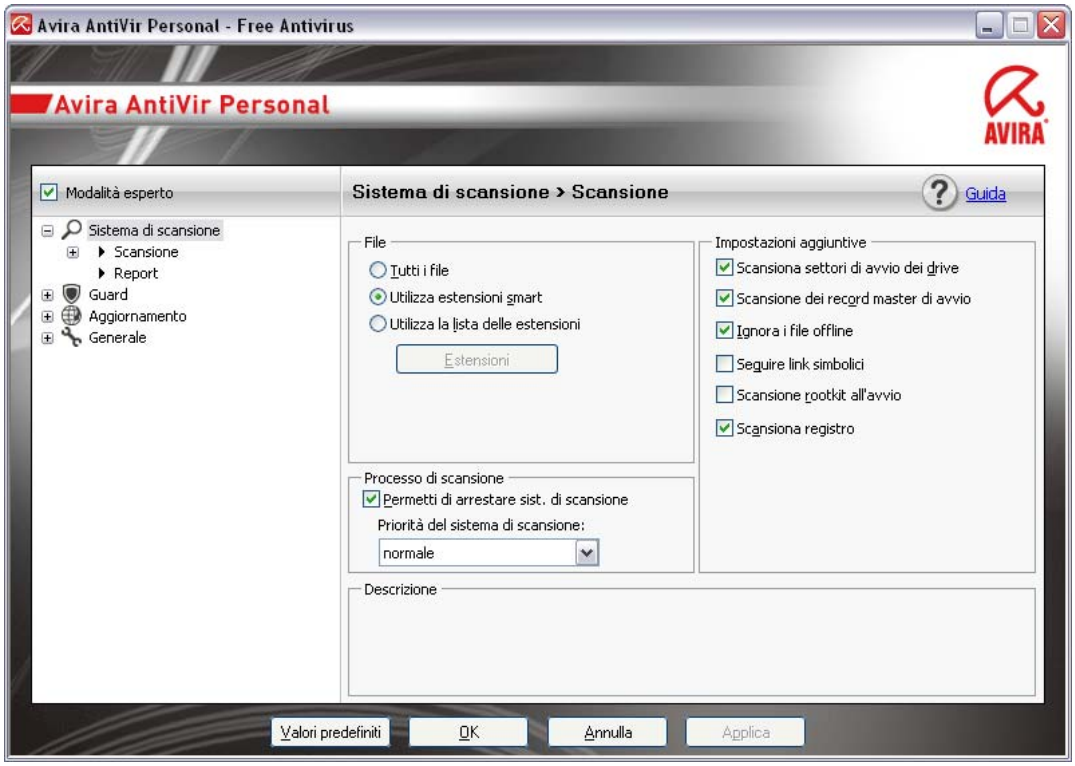
Control Center in sintesi

- **Panoramica**: in **Panoramica** sono disponibili tutte le rubriche che consentono di monitorare le funzionalità di Avira AntiVir Personal.

- La rubrica **Stato** offre la possibilità di visualizzare quali moduli di Avira AntiVir Personal sono attivi e fornisce informazioni sull'ultimo aggiornamento effettuato. Inoltre, è possibile verificare se si possiede una licenza valida.
- La rubrica Eventi consente di ottenere informazioni sugli eventi generati dai moduli di Avira AntiVir Personal.
- La rubrica Report consente di visualizzare i risultati delle azioni eseguite da Avira AntiVir Personal.
- **Protezione locale**: in **Protezione locale** sono disponibili i componenti con cui eseguire la ricerca di virus e malware nei file del computer.
- La rubrica Scansiona offre la possibilità di configurare o avviare la scansione diretta in modo semplice. I profili predefiniti consentono una scansione con le opzioni standard già adeguate. Con l'aiuto della Selezione manuale (non viene memorizzata) è possibile adattare la scansione di virus e programmi indesiderati alle proprie esigenze personali.
- La rubrica Guard visualizza informazioni su file scansionati, così come ulteriori dati statistici, che possono essere ripristinati in qualsiasi momento e permette il richiamo del file di report. Informazioni dettagliate sull'ultimo virus o programma indesiderato trovato sono reperibili "premendo un pulsante".
- **Gestione**: in **Gestione** sono disponibili gli strumenti che consentono di isolare e gestire file sospetti o infetti nonché pianificare attività ricorrenti.
- Nella rubrica Quarantena è disponibile il cosiddetto Gestore della quarantena, la postazione centrale per i file già in quarantena o per file sospetti che si desidera spostare in quarantena. Inoltre esiste la possibilità di inviare un file selezionato per email all'Avira Malware Research Center.
- La rubrica Scheduler offre la possibilità di creare job temporizzati di controllo e di aggiornamento e di cancellare o modificare job esistenti.

5.1.2 Configurazione

In Configurazione è possibile effettuare le impostazioni per AntiVir Personal. Dopo l'installazione, AntiVir Personal è configurato con le impostazioni standard che assicurano la protezione ottimale del computer. Ciononostante, il computer o le richieste dell'utente per AntiVir Personal possono possedere caratteristiche particolari e richiedere un adattamento delle componenti di protezione di AntiVir Personal.



La configurazione dispone di una finestra di dialogo: con i pulsanti OK o Applica si memorizzano le impostazioni scelte durante la configurazione, con Annulla si rifiutano le impostazioni, con il pulsante Valori standard è possibile ripristinare le impostazioni dei valori standard della configurazione. Nella barra di navigazione a sinistra è possibile selezionare singole rubriche di configurazione.

Richiamo della Configurazione di AntiVir Personal

Esistono diverse possibilità per richiamare la configurazione:

- Mediante il pannello di controllo di Windows .
- Mediante il centro sicurezza di Windows - a partire da Windows XP Service Pack 2.
- Mediante la Icona Tray di Avira AntiVir Personal.
- Nel Control Center di Avira AntiVir Personal mediante la voce di menu Extra | Configurazione.
- Nel Control Center di Avira AntiVir Personal mediante il pulsante Configurazione.

Nota
Se si richiama la configurazione con il pulsante **Configurazione** in Control Center, si giunge nel registro di configurazione della categoria attiva in Control Center. Per selezionare un singolo registro di configurazione, è necessario attivare la modalità esperto della configurazione. In questo caso appare una finestra di dialogo, in cui viene richiesto di attivare la modalità esperto.

Utilizzo della Configurazione

All'interno della finestra di configurazione si può navigare come in Esplora risorse di Windows:

- ▶ Fare clic su una voce della struttura ad albero per visualizzare questa categoria di configurazione nella finestra dei dettagli.

- Fare clic sul segno + prima delle voci per estendere la categoria di configurazione e visualizzare le rubriche di configurazione subordinate nella struttura ad albero.
- Per nascondere le rubriche di configurazione subordinate fare clic sul segno - prima della categoria di configurazione estesa.

Nota
Per attivare o disattivare le opzioni nella configurazione e per premere i pulsanti è possibile utilizzare anche le seguenti combinazioni di tasti: tasto [Alt] + lettera sottolineata nei nomi opzione o nella definizione pulsanti.

Nota
Le rubriche di configurazione vengono visualizzate per intero nella modalità esperto. Attivare la modalità esperto per visualizzare tutte le rubriche di configurazione. La modalità esperto può essere protetta con una password da digitare al momento dell'attivazione.

Se si desidera registrare le impostazioni nella configurazione:

- Fare clic sul pulsante **OK**.

→ La finestra di configurazione viene chiusa e le impostazioni registrate.

- OPPURE -

- Fare clic sul pulsante **Applica**.

→ Le impostazioni vengono registrate. La finestra di configurazione rimane aperta.

Se si desidera terminare la configurazione senza memorizzare le impostazioni:

- Fare clic sul pulsante **Annulla**.

→ La finestra di configurazione si chiude e le impostazioni vengono ignorate.

Se si desidera ripristinare tutte le impostazioni dei valori standard nella configurazione:

- Fare clic su **Valori standard**.

→ Tutte le impostazioni dei valori standard nella configurazione vengono ripristinate. Quando si ripristinano i valori standard tutte le modifiche e le immissioni dell'utente vengono perse.

Opzioni di configurazione in sintesi

Esistono le seguenti opzioni di configurazione:

- **Sistema di scansione**: Configurazione della scansione diretta
  - Opzioni di ricerca
  - Azioni in caso di rilevamento
  - Opzioni per la scansione degli archivi
  - Eccezioni della scansione diretta
  - Euristica della scansione diretta
  - Impostazione della funzione di report
- **Guard**: Configurazione della scansione in tempo reale
  - Opzioni di ricerca
  - Azioni in caso di rilevamento
  - Eccezioni della scansione in tempo reale
  - Euristica della scansione in tempo reale
  - Impostazione della funzione di report

– **Generale**:

Configurazione dell'invio di email mediante SMTP

Categorie estese delle minacce per la scansione diretta e in tempo reale

Sicurezza: indicatore di stato aggiornamento, indicatore di stato scansione completa del sistema, protezione del prodotto

WMI: attiva supporto WMI

Configurazione del log eventi

Configurazione delle funzioni di report

Impostazione delle directory utilizzate

Aggiornamento: configurazione del collegamento al server di download, impostazione dell'aggiornamento del prodotto

Configurazione degli avvisi acustici in caso di rilevamento malware

5.1.3 Icona Tray

Dopo l'installazione, l'icona Tray di AntiVir Personal è collocata nella barra delle applicazioni:

Simbolo	Descrizione
	AntiVir Guard è attivato
	AntiVir Guard è disattivato

L'icona Tray mostra lo stato del servizio AntiVir Guard.

Le funzioni principali di Avira AntiVir Personal sono facilmente accessibili mediante il menu contestuale dell'icona Tray. Per richiamare il menu contestuale, fare clic con il tasto destro del mouse sull'icona Tray.

Voci del menu contestuale

– **Attiva AntiVir Guard**: attiva o disattiva Avira AntiVir Guard.
– **Avvia AntiVir**: Apre Control Center di Avira AntiVir Personal .
– **Configura AntiVir**: Apre Configurazione.
– **Avvia aggiornamento**: Avvia un aggiornamento.
– **Guida in linea**: Apre questa guida in linea.
– **Avira su Internet**: Apre il portale Web del produttore di AntiVir Personal in Internet. Il prerequisito essenziale è l'accesso attivo a Internet.

5.2 Come procedere

5.2.1 Aggiornare automaticamente Avira AntiVir Personal

Per impostare con AntiVir Scheduler un job con cui aggiornare automaticamente Avira AntiVir Personal:

▶ Selezionare la rubrica **Gestione::Scheduler** in Control Center.

- Fare clic sul simbolo *Crea nuovo job con wizard*.
- Appare la finestra di dialogo *Nome e descrizione del job*.
- Assegnare un nome al job e descriverlo.
- Fare clic su **Avanti**.
- Viene visualizzata la finestra di dialogo *Tipo di job*.
- Selezionare un **Job di aggiornamento** dalla lista.
- Fare clic su **Avanti**.
- Apparirà la finestra di dialogo *Durata del job*.
- Selezionare quando deve essere eseguita la scansione:
  - **Immediato**
  - **Giornaliero**
  - **Settimanale**
  - **Intervallo**
  - **Unico**

Nota
Suggeriamo di aggiornare regolarmente e spesso Avira AntiVir Personal. L'intervallo di aggiornamento consigliato è: 24 Ore.

- Indicare il termine in base alla selezione.
- Selezionare una delle seguenti opzioni aggiuntive (disponibili in base al tipo di job):
  - **Ripeti job se il tempo è scaduto**

    Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.
- Fare clic su **Avanti**.
- Appare la finestra di dialogo *Selezione della modalità di visualizzazione* .
- Selezionare la modalità di visualizzazione della finestra del job:
  - **Ridotta**: solo la barra di progressione
  - **Estesa**: tutta la finestra del job
  - **Invisibile**: nessuna finestra del job
- Fare clic su **Fine**.
- Il nuovo job assegnato viene visualizzato alla pagina iniziale della rubrica **Gestione :: Scansiona** come attivato (segno di spunta).
- Disattivare i job che non devono essere eseguiti.

Mediante i seguenti simboli, è possibile elaborare ulteriormente i job:

Visualizza le proprietà di un job

Modifica job

Elimina job

Avvia job

Arresta job

5.2.2 Avvio di un aggiornamento manuale

Sono disponibili varie opzioni per avviare manualmente un aggiornamento di Avira AntiVir Personal: durante gli aggiornamenti avviati manualmente viene sempre eseguito anche l'aggiornamento del file di definizione dei virus e del motore di ricerca. L'aggiornamento del prodotto avviene soltanto se nella configurazione in Generale :: Aggiornamento è stata attivata l'opzione **Scarica aggiornamenti del prodotto e installa automaticamente**.

Per avviare manualmente un aggiornamento di Avira AntiVir Personal:

- ▶ Fare clic con il tasto destro del mouse sull'icona Tray di Avira AntiVir Personal nella barra delle applicazioni.
- → Apparirà un menu contestuale.
- ▶ Selezionare **Avvia aggiornamento**.
- → Appare la finestra di dialogo *Updater*.

- OPPURE -

- ▶ Selezionare la rubrica **Panoramica :: Stato** in Control Center.
- ▶ Fare clic nella sezione *Ultimo aggiornamento* sul link **Avvia aggiornamento**.
- → Appare la finestra di dialogo Updater.

- OPPURE -

- ▶ In Control Center, nel menu **Aggiornamento** selezionare il comando *Avvia aggiornamento*.
- → Appare la finestra di dialogo Updater.

Nota
Suggeriamo di aggiornare regolarmente Avira AntiVir Personal. L'intervallo di aggiornamento consigliato è: 24 Ore.

Nota
É possibile eseguire un aggiornamento anche manualmente mediante il Centro di sicurezza Windows.

5.2.3 Scansione diretta: Eseguire il controllo di virus e malware con un profilo di ricerca

Un profilo di ricerca è un insieme di drive e directory che devono essere scansionati.

Per effettuare una scansione con un profilo di ricerca è possibile:

- Utilizzare il profilo di ricerca predefinito

  Se i profili di ricerca predefiniti si adattano alle proprie esigenze.

- Modificare il profilo di ricerca e utilizzarlo (selezione manuale)

  Se si desidera eseguire una scansione con un profilo di ricerca personalizzato.

In base al sistema operativo sono disponibili diversi simboli per l'avvio di un profilo di ricerca:

- In Windows XP e 2000:

  Con questo simbolo si avvia la scansione mediante un profilo di ricerca.

- In Windows Vista:

In Microsoft Windows Vista il Control Center ha inizialmente diritti limitati ad esempio per l'accesso a file e directory. Alcune azioni e l'accesso ai file possono essere eseguiti dal Control Center solo con diritti di amministratore avanzati. Questi diritti di amministratore avanzati devono essere assegnati a ogni avvio di una scansione mediante un profilo di scansione.

Con questo simbolo si avvia una scansione limitata mediante un profilo di ricerca. Vengono scansionati solo i file e le directory per cui Windows Vista ha concesso i diritti di accesso.

Con questo simbolo si avvia una scansione con diritti avanzati dell'amministratore. Dopo una conferma, vengono scansionati tutti i file e le directory del profilo di ricerca selezionato.

Per cercare virus e malware con un profilo:

- ▶ Selezionare la rubrica **Protezione locale :: Scansiona** nel Control Center.
- ➔ Appaiono i profili di ricerca predefiniti.
- ▶ Selezionare un profilo di ricerca predefinito.

  - OPPURE -
- ▶ Modificare il profilo di ricerca in *Selezione manuale*.
- ▶ Fare clic sul simbolo (Windows XP: o Windows Vista:).
- ▶ Appare la finestra *Luke Filewalker* e si avvia la scansione diretta.
- ➔ Al termine del processo di scansione vengono visualizzati i risultati.

Se si desidera modificare un profilo di ricerca:

- ▶ Aprire nel profilo di ricerca **Selezione manuale** la struttura dei file fin quando non vengono aperti tutti i drive che devono essere scansionati:
- ▶ Selezionare i punti che devono essere scansionati facendo clic nella casella:

5.2.4 Scansione diretta: Ricerca di virus e malware con Drag&Drop

È possibile cercare con Drag&Drop virus e malware come segue:

- ✓ Il Control Center di Avira AntiVir Personal si apre.
- ▶ Selezionare il file, che si desidera controllare.
- ▶ Trascinare con il tasto sinistro del mouse il file selezionato in *Control Center*.
- ➔ Appare la finestra *Luke Filewalker* e si avvia la scansione diretta.
- ➔ Al termine del processo di scansione vengono visualizzati i risultati.

5.2.5 Scansione diretta: Ricerca di virus e malware con il menu contestuale

Per cercare in maniera mirata virus e malware mediante il menu contestuale:

- ▶ Fare clic (ad esempio in Esplora risorse di Windows, sul desktop o in una directory aperta di Windows) con il tasto destro del mouse sul file chesi desidera controllare.
- ➔ Appare il menu contestuale di Esplora risorse di Windows.
- ▶ Nel menu contestuale selezionare **Controlla i file selezionati con AntiVir**.

→ Appare la finestra *Luke Filewalker* e si avvia la scansione diretta.

→ Al termine del processo di scansione vengono visualizzati i risultati.

5.2.6 Scansione diretta: Cercare automaticamente virus e malware

Nota
Una volta eseguita l'installazione il job *Scansione completa del sistema* si trova nello Scheduler: in un intervallo di aggiornamento consigliato viene eseguita automaticamente una scansione completa del sistema.

Cercare automaticamente virus e malware è un job che si imposta come segue:

▶ Selezionare la rubrica **Gestione :: Scheduler** in Control Center.

▶ Fare clic sul simbolo

→ Appare la finestra di dialogo *Nome e descrizione del job*.

▶ Assegnare un nome al job e descriverlo.

▶ Fare clic su **Avanti**.

→ Appare la finestra di dialogo *Tipo di job*.

▶ Selezionare il **Job di scansione**.

▶ Fare clic su **Avanti**.

→ Appare la finestra di dialogo *Selezione del profilo*.

▶ Selezionare quale profilo deve essere scansionato.

▶ Fare clic su **Avanti**.

→ Apparirà la finestra di dialogo *Durata del job*.

▶ Selezionare quando deve essere eseguita la scansione:

- **Immediato**
- **Giornaliero**
- **Settimanale**
- **Intervallo**
- **Unico**

▶ Indicare il termine in base alla selezione.

▶ Selezionare una delle seguenti opzioni aggiuntive (disponibili in base al tipo di job):

- **Ripeti job se il tempo è scaduto**

  Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.

▶ Fare clic su **Avanti**.

→ Appare la finestra di dialogo *Selezione della modalità di visualizzazione* .

▶ Selezionare la modalità di visualizzazione della finestra del job:

- **Ridotta**: solo la barra di progressione
- **Estesa**: tutta la finestra del job
- **Invisibile**: nessuna finestra del job

▶ Selezionare l'opzione *Spegni computer*, se si desidera che il calcolatore si spenga automaticamente non appena il job è stato eseguito e concluso. L'opzione è disponibile solo nella modalità di visualizzazione ridotta o estesa.

▶ Fare clic su **Fine**.

→ Il nuovo job assegnato viene visualizzato alla pagina iniziale della rubrica *Gestione :: Scheduler* come attivato (segno di spunta).

▶ Disattivare i job che non devono essere eseguiti.

Mediante i seguenti simboli, è possibile elaborare ulteriormente i job:

Visualizza proprietà di un job

Modifica job

Elimina job

Avvia job

Arresta job

5.2.7 Scansione diretta: Effettuare una scansione mirata per rootkit attivi

Per effettuare una scansione per rootkit attivi utilizzare il profilo di scansione predefinito *Cerca rootkit*.

La ricerca di rootkit mirata si effettua nel modo seguente:

▶ Selezionare la rubrica **Protezione locale :: Scansiona** nel Control Center.

→ Appaiono i profili di ricerca predefiniti.

▶ Selezionare il profilo di ricerca predefinito **Cerca malware attivi**.

▶ Evidenziare altri punti e directory che devono essere verificati con un clic nella casella del livello della directory.

▶ Fare clic sul simbolo (Windows XP: o Windows Vista:).

→ Appare la finestra *Luke Filewalker* e si avvia la scansione diretta.

→ Al termine del processo di scansione vengono visualizzati i risultati.

5.2.8 Reagire a virus e malware riscontrati

Per i singoli componenti di protezione di AntiVir Personal è possibile impostare nella configurazione, nella rubrica *Azione in caso di rilevamento*, come AntiVir Personal deve reagire al rilevamento di un virus o di un programma indesiderato.

Nel componente Guard non esiste la possibilità di configurare alcuna opzione di azione. In caso di rilevamento di un virus compare un messaggio sul desktop. È possibile rimuovere il malware rilevato direttamente nel messaggio sul desktop, oppure trasmettere il malware al componente Scanner per un ulteriore trattamento del virus selezionando il pulsante 'Dettagli'. Il sistema di scansione segnala il rilevamento in una finestra, nella quale, mediante un menu contestuale, sono disponibili diverse opzioni per il trattamento del file infetto (vedere Rilevamento::Scanner).

Opzioni di azione in Scanner:

– **Interattivo**

Nella modalità di azione interattiva vengono notificati i rilevamenti della scansione di Scanner in una finestra di dialogo. Questa opzione è attivata di default.
Al termine della **scansione di Scanner**, si riceve un avviso con l'elenco dei file infetti rilevati. Mediante il menu contestuale è possibile selezionare un'azione da eseguire per i singoli file infetti. È possibile eseguire l'azione selezionata per tutti i file infetti oppure interrompere la scansione.

– **Automatico**

Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Opzioni di azione in :

– **Interattivo**

Nella modalità di azione interattiva, in caso di rilevamento di un virus o di un programma indesiderato appare una finestra di dialogo nella quale è possibile scegliere come gestire i file infetti. Questa opzione è attivata di default.

– **Automatico**

Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Nella modalità di azione interattiva si reagisce ai virus e ai programmi indesiderati rilevati selezionando nell'avviso un'azione per gli oggetti infetti ed eseguendo l'azione selezionata mediante conferma.

Per il trattamento di oggetti infetti possono essere selezionate le seguenti azioni:

Nota
Le azioni disponibili dipendono dal sistema operativo, dal componente di protezione (AntiVir Guard, AntiVir Scanner) che segnala il file rilevato, e dal malware rilevato.

Azioni di Scanner e di Guard:

– **Ripara**

Il file viene riparato.

Questa opzione è attivabile solo se è possibile riparare il file.

– **Sposta in quarantena**

Il file viene compresso in un formato speciale (*.*qua*) e spostato nella directory di quarantena *INFECTED* sull'hard disk, in modo da escludere qualsiasi accesso diretto. I file in questa directory possono essere successivamente riparati nella quarantena o, se necessario, inviati a Avira GmbH.

– **Elimina**

Il file viene eliminato. Se il file rilevato è un virus del record di avvio eliminarlo con Elimina. Viene scritto un nuovo record di avvio.

– **Rinomina**

Il file viene rinominato *.*vir*. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere successivamente riparati e nuovamente rinominati.

– **Ignora**

Avira AntiVir Personal non esegue alcuna altra azione. Il file infetto rimane attivo sul computer.

Attenzione
Pericolo di perdita di dati e danni al sistema operativo! Utilizzare l'opzione *Ignora* solo in casi eccezionali e fondati.

- **Nega accesso**

  Opzione di azione in caso di file rilevati da Guard: l'accesso al file infetto viene bloccato. Il file rilevato viene inserito nel file di report (se la funzione di report è attivata).

- **Copia in quarantena**

  Opzione di azione in caso di rilevamento di un rootkit: il file rilevato viene copiato nella quarantena.

- **Ripara record di avvio | Scarica strumento di riparazione**

  Opzioni di azione in caso di rilevamento di record di avvio infetto: in caso di drive del floppy disk infetti sono disponibili opzioni per effettuare la riparazione con AntiVir Personal. Se con AntiVir Personal non è possibile effettuare alcuna riparazione, è possibile scaricare uno strumento speciale che riconosce e rimuove i virus del record di avvio.

Nota
Se si applicano azioni su processi in corso, i processi interessati vengono terminati prima dell'esecuzione dell'azione.

Nota
Consigliamo di spostare in quarantena un file sospetto che non può essere riparato.

5.2.9 Quarantena: Trattare file (*.qua) in quarantena

É possibile trattare i file in quarantena nel modo seguente:

- Selezionare la rubrica **Gestione :: Quarantena** in Control Center.
- Verificare di quali file si tratta cosicché sia possibile ripristinare gli originali sul computer.

Se si desidera visualizzare maggiori informazioni su un file:

- Selezionare il file e fare clic su

→ Apparirà la finestra di dialogo *Proprietà* con ulteriori informazioni sul file.

Se si desidera verificare nuovamente un file:

La verifica di un file è consigliata quando il file di definizione dei virus di Avira AntiVir Personal è stato aggiornato ed esiste il sospetto di un falso allarme. É così possibile confermare un falso allarme a una successiva verifica e ripristinare il file.

- Selezionare il file e fare clic su

→ Il file viene controllato utilizzando le impostazioni della scansione diretta per virus e malware.

→ Dopo il controllo appare la finestra di dialogo *Statistiche della scansione* che visualizza la statistica relativa allo stato del file prima e dopo la nuova scansione.

Se si desidera eliminare un file:

- Selezionare il file e fare clic su

Se si desidera caricare il file da analizzare su un server Web di Avira Malware Research Center:

- Selezionare il file che si desidera caricare.
- Fare clic su

→ Si aprirà una finestra di dialogo con un modulo per inserire i dati personali a cui essere contattati.

- Indicare per intero i propri dati.
- Selezionare un tipo: **File sospetto** o **Falso allarme**.
- Fare clic su **OK.**

→ Il file compresso viene caricato su un server Web di Avira Malware Research Center.

Nota
Nei seguenti casi si consiglia un'analisi da parte di Avira Malware Research Center:
Oggetto euristico (file sospetto): Durante una scansione un file di AntiVir Personal è stato identificato come sospetto e spostato in quarantena: Nella finestra di dialogo per il rilevamento di virus o nel file di report della scansione è stata consigliata l'analisi del file da parte di Avira Malware Research Center.

Nota
La dimensione dei file caricati si limita a 20 MB non compressi o a 8 MB compressi.

Nota
È possibile caricare solo un singolo file per volta.

Se si desidera esportare in un file di testo le proprietà di un oggetto in quarantena selezionato:

- Selezionare il file in quarantena e fare clic su

→ Si apre un file di testo con i dati dell'oggetto in quarantena scelto.

- Salvare il file di testo.

I file in quarantena possono anche essere ripristinati:

– vedere capitolo: Quarantena: Ripristinare file in quarantena

5.2.10 Quarantena: Ripristinare file in quarantena

In base al sistema operativo sono disponibili diversi sistemi per il ripristino:

– In Windows XP e 2000:

Con questo simbolo si ripristinano i file nella directory originale.

Con questo simbolo si ripristinano i file nella directory selezionata.

– In Windows Vista:

In Microsoft Windows Vista il Control Center ha inizialmente diritti limitati ad esempio per l'accesso a file e directory. Alcune azioni e l'accesso ai file possono essere eseguiti dal Control Center solo con diritti di amministratore avanzati. Questi diritti di amministratore avanzati devono essere assegnati a ogni avvio di una scansione mediante un profilo di scansione.

Con questo simbolo si ripristinano i file nella directory selezionata.

Con questo simbolo si ripristinano i file nella directory originale. Se per l'accesso a questa directory sono necessari diritti di amministratore avanzati, appare una richiesta corrispondente.

É possibile ripristinare i file in quarantena nel modo seguente:

Attenzione
Pericolo di perdita di dati e danni al sistema operativo del computer! Utilizzare la funzione *Ripristina l'oggetto selezionato* solo in casi eccezionali. Ripristinare solo quei file che possono essere riparati con una nuova scansione.

✓ File nuovamente controllato e riparato con una scansione.

▶ Selezionare la rubrica **Gestione :: Quarantena** in Control Center.

Nota
Le email e gli allegati possono essere ripristinati solo con l'opzione e con l'estensione **.eml*.

Se si desidera ripristinare un file nella sua posizione originale:

▶ Evidenziare il file e fare clic sul simbolo (Windows 2000/XP: , Windows Vista).

Questa opzione non è disponibile per le email.

Nota
Le email e gli allegati possono essere ripristinati solo con l'opzione e con l'estensione **.eml*.

→ Viene richiesto quindi se si desidera ripristinare il file.

▶ Fare clic su **Sì**.

→ Il file viene ripristinato nella directory dalla quale è stato spostato in quarantena.

Se si desidera ripristinare un file in una determinata directory:

▶ Selezionare il file e fare clic su

→ Viene richiesto quindi se si desidera ripristinare il file.

▶ Fare clic su **Sì**.

→ Apparirà la finestra standard di Windows per la selezione di una directory.

▶ Selezionare la directory nella quale si desidera ripristinare il file e confermare.

→ Il file viene ripristinato nella directory selezionata.

5.2.11 Quarantena: Spostare i file sospetti in quarantena

É possibile spostare in quarantena i file sospetti manualmente come segue:

▶ Selezionare la rubrica **Gestione :: Quarantena** in Control Center.

▶ Fare clic su

→ Apparirà la finestra standard di Windows per la selezione di un file.

▶ Selezionare il file e confermare.

→ Il file viene spostato in quarantena.

É possibile controllare i file in quarantena con AntiVir Scanner:

- vedere capitolo: Quarantena: Trattare file (*.qua) in quarantena

5.2.12 Profilo di ricerca: Inserire o eliminare un tipo di file in un profilo di ricerca

Per stabilire per un profilo di ricerca i tipi di file da scansionare o i tipi di file che devono essere esclusi dalla ricerca (possibile solo con selezione manuale):

✓ Dalla rubrica **Protezione locale ::** *Scansiona* nel Control Center,

▶ fare clic con il tasto destro del mouse sul profilo di ricerca che si desidera modificare.

→ Apparirà un menu contestuale.

▶ Selezionare la voce **Filtro file**.

▶ Aprire nuovamente il menu contestuale facendo clic sul piccolo triangolo sul lato destro del menu contestuale.

→ Appariranno le voci *Standard*, *Controlla tutti i file* e *Personalizzato*.

▶ Selezionare la voce **Personalizzato**.

→ Apparirà la finestra di dialogo *Estensione file* con un elenco di tutti i tipi di file che devono essere abbinati al profilo di ricerca.

Se si desidera escludere un tipo di file dalla scansione:

▶ Selezionare il tipo di file e fare clic su **Elimina**.

Se si desidera aggiungere un tipo di file dalla scansione:

▶ Selezionare il tipo di file.

▶ Fare clic su **Aggiungi** e inserire l'estensione del tipo di file nel campo.

Utilizzare un massimo di 10 caratteri e non inserire punti. I metacaratteri (* e ?) sostitutivi sono consentiti.

5.2.13 Profilo di ricerca: Creare un collegamento sul desktop per il profilo di ricerca

Mediante un collegamento sul desktop per un profilo di ricerca è possibile avviare una scansione diretta facendo clic sul desktop senza richiamare il Control Center di Avira AntiVir Personal.

É possibile creare un collegamento al profilo di ricerca dal desktop:

✓ Dalla rubrica **Protezione locale ::** *Scansiona* nel Control Center,

▶ selezionare il profilo di ricerca di cui si intende creare il collegamento.

▶ Fare clic sul simbolo

→ Viene creato un collegamento sul desktop.

5.2.14 Eventi: filtrare eventi

In **Panoramica :: Eventi** vengono visualizzati eventi creati dai componenti del programma di AntiVir Personal. (analogamente al visualizzatore eventi del sistema operativo di Windows). Le componenti del programma sono:

- Updater
- Guard
- Sistema di scansione
- Scheduler

Vengono visualizzati i seguenti tipi di eventi:

- Informazioni
- Attenzione
- Errore
- Rilevamento

Come filtrare gli eventi visualizzati:

- Selezionare la rubrica **Panoramica :: Backup** in Control Center.
- Attivare la casella delle componenti di programma per visualizzare gli eventi delle componenti attive.

  - OPPURE -

  Disattivare la casella delle componenti di programma per non visualizzare gli eventi delle componenti disattivate.

- Attivare la casella dei tipi di evento per visualizzare questi eventi.

  - OPPURE -

  Disattivare la casella dei tipi di evento per non visualizzare questi eventi.

6 Scanner

Con il componente Scanner è possibile effettuare scansioni mirate per virus e programmi indesiderati (scansione diretta). È possibile effettuare una scansione per file infetti in diversi modi:

- **Scansione diretta mediante menu contestuale**
  La scansione diretta mediante il menu contestuale (tasto destro del mouse - voce **Controlla i file selezionati con AntiVir**) si consiglia quando, ad esempio, si desidera controllare singoli file e directory in Esplora risorse di Windows. Un ulteriore vantaggio è che Control Center di Avira AntiVir Personal non deve essere avviato per la scansione diretta mediante il menu contestuale.
- **Scansione diretta con Drag & Drop**
  Trascinando un file o una directory nella finestra di programma del Control Center di Avira AntiVir Personal Scanner verifica il file o la directory, nonché tutte le sottodirectory. Questa procedura è consigliata quando si desidera controllare i singoli file e directory che sono stati archiviati, ad esempio, sul desktop.
- Scansione diretta per profili
  Questa procedura è consigliata quando si desidera controllare regolarmente alcune directory e drive (ad esempio la propria directory di lavoro o drive, sui quali si archiviano regolarmente nuovi file). Queste directory e drive non devono quindi essere selezionati a ogni scansione ma vengono comodamente selezionati tramite il profilo corrispondente.
- **Scansione diretta con Scheduler**
  Scheduler offre la possibilità di far eseguire job temporizzati di scansione.

Durante la scansione per rootkit, virus del record di avvio e la scansione dei processi attivi sono necessari dei procedimenti particolari. Sono disponibili le seguenti opzioni:

- Scansione di rootkit mediante il profilo di ricerca *Scansiona rootkit*
- Scansione dei processi attivi mediante il profilo di ricerca **Processi attivi**
- Scansiona virus del record di avvio con il comando **Scansiona virus del record di avvio** nel menu **Extra**

7 Aggiornamenti

L'efficacia di un software antivirus dipende dall'aggiornamento del programma, in particolare del file di definizione dei virus e del motore di ricerca. Per l'esecuzione degli aggiornamenti, il componente Updater è integrato in AntiVir Personal. Updater garantisce che Avira AntiVir Personal sia sempre il più aggiornato possibile e che sia in grado di rilevare i nuovi virus che compaiono quotidianamente. Updater aggiorna i seguenti componenti:

- File di definizione dei virus:

  Il file di definizione dei virus contiene il modello di rilevamento del programma dannoso che AntiVir Personal utilizza nella scansione per virus e malware nonché nella riparazione di oggetti infetti.

- Motore di ricerca:

  Il motore di ricerca contiene i metodi che vengono utilizzati da AntiVir Personal per la scansione per virus e malware.

- File di programma (aggiornamento del prodotto):

  I pacchetti di aggiornamento del prodotto mettono a disposizione ulteriori funzioni per i singoli componenti del programma.

Durante un aggiornamento viene verificato lo stato di aggiornamento del file di definizione dei virus e del motore di ricerca e, se necessario, tali componenti vengono aggiornati. In base alle impostazioni di configurazione Updater esegue un aggiornamento del prodotto o segnala la disponibilità di tale aggiornamento. Terminato un aggiornamento del prodotto può essere necessario riavviare il sistema. Se l'aggiornamento avviene solo per il file di definizione dei virus e del motore di ricerca non è necessario riavviare il computer.

Nota
Per motivi di sicurezza, Updater verifica se il file host di Windows del computer è stato modificato, ad esempio con manipolazione da parte di malware dell'URL di aggiornamento per Avira AntiVir Personal a seguito della quale Updater viene indirizzato a pagine di download indesiderate. Se il file host di Windows è stato manipolato, l'evento viene riportato nel file di record di Updater.

Un aggiornamento di AntiVir Personal viene eseguito in automatico nel seguente intervallo: 24 Ore. È possibile modificare o disattivare l'aggiornamento automatico dalla configurazione (Configurazione::Aggiorna).

In Control Center in Scheduler è possibile configurare ulteriori job di aggiornamento che Updater deve eseguire a intervalli definiti. È inoltre possibile avviare l'aggiornamento manualmente:

- In Control Center: nel menu Aggiornamento e della rubrica Stato
- Tramite il menu contestuale dell'icona Tray

Gli aggiornamenti vengono richiamati da Internet tramite un server Web del produttore. Normalmente si utilizza la connessione di rete esistente per collegarsi al server di download di Avira GmbH. Questa impostazione standard può essere modificata nella configurazione in Generale :: Aggiorna.

8 FAQ, suggerimenti

In questo capitolo è possibile consultare le domande frequenti relative a Avira AntiVir Personal, la guida in linea per problemi, nonché suggerimenti e accorgimenti inerenti a Avira AntiVir Personal.

Vedere capitolo Assistenza in caso di problemi

Vedere capitolo Shortcut

Vedere capitolo Centro sicurezza di Windows

8.1 Assistenza in caso di problemi

Qui sono reperibili informazioni sulle cause e le soluzioni di eventuali problemi.

Il messaggio di errore *Lo stabilimento della connessione è fallito durante il download del file ...* viene visualizzato nel tentativo di avviare un aggiornamento.

Causa: la connessione Internet non è attiva. Pertanto Avira AntiVir Personal non trova il server Web su Internet.

▶ Provare se altri servizi Internet come WWW o l'email funzionano. Se non funzionano ripristinare la connessione Internet.

Causa: il server proxy non è raggiungibile.

▶ Verificare se sia cambiato il login per il server proxy e adattare eventualmente la propria configurazione.

Causa: il file update.exe non è ammesso dal proprio firewall.

▶ Assicurarsi che il file update.exe sia ammesso dal proprio firewall.

Altrimenti:

▶ Controllare le impostazioni nella configurazione (modalità esperto) in Generale :: Aggiornamento.

Impossibile spostare o eliminare virus e malware.

Causa: il file è stato caricato da Windows ed è attivo.

▶ Aggiornare Avira AntiVir Personal.

▶ Se si utilizza il sistema operativo Windows XP, disattivare il ripristino del sistema.

▶ Avviare il computer in modalità provvisoria.

▶ Avviare Avira AntiVir Personal e la configurazione (modalità esperto).

▶ Selezionare Sistema di scansione :: Scansione :: File :: Tutti i file e confermare la finestra con **OK**.

▶ Avviare una scansione su tutti i drive locali.

▶ Avviare il computer in modalità normale.

▶ Eseguire una scansione in modalità normale.

▶ Se non vengono rilevati altri virus e malware attivare il ripristino del sistema se è disponibile e deve essere utilizzato.

L'icona Tray mostra uno stato disattivato.

Causa: AntiVir Guard è disattivato.

▶ Nel Control Center fare clic nella rubrica Panoramica :: Stato nella sezione AntiVir Guard sul link **Attiva**.

Causa: AntiVir Guard è bloccato da un firewall.

▶ Nella configurazione del firewall definire un permesso generale per AntiVir Guard. AntiVir Guard lavora esclusivamente con l'indirizzo 127.0.0.1 (localhost). Non viene stabilita alcuna connessione Internet.

Altrimenti:

▶ Verificare la modalità di attivazione del servizio AntiVir Guard. Attiva eventualmente il servizio: selezionare in "Start | Impostazioni | Pannello di controllo". Avviare il pannello di configurazione "Servizi" con un doppio clic (in Windows 2000 e Windows XP l'applet servizi si trova nella sottodirectory "Gestione"). Cercare la voce "Avira AntiVir Guard". Come modalità di avviamento deve essere inserito "Automatico" e come stato "Avviato". Avviare il servizio manualmente mediante la selezione della riga corrispondente e del pulsante "Avvia". Se viene visualizzato un messaggio di errore, verificare la visualizzazione eventi.

Il computer diventa estremamente lento se eseguo un backup.

Causa: AntiVir Guard scansiona tutti i dati con i quali lavora il backup durante il processo di backup.

▶ Selezionare nella configurazione (modalità esperto) Guard :: Scansione :: Eccezioni e inserire il nome del processo del software di backup.

Il mio firewall segnala AntiVir Guard se sono attivi.

Causa: la comunicazione di AntiVir Guard avviene mediante il protocollo Internet TCP/IP. Un firewall monitora tutte le connessioni mediante questo protocollo.

▶ Definire un permesso generale per AntiVir Guard. AntiVir Guard lavora esclusivamente con l'indirizzo 127.0.0.1 (localhost). Non viene stabilita alcuna connessione Internet.

Nota
Consigliamo di eseguire regolarmente gli aggiornamenti Microsoft per colmare le eventuali lacune in termini di sicurezza.

8.2 Shortcut

Le shortcut offrono la possibilità di navigare velocemente in Avira AntiVir Personal, richiamare singoli moduli e avviare azioni.

Di seguito viene presentata una panoramica delle shortcut presenti in Avira AntiVir Personal. Per maggiori informazioni sulla funzionalità e disponibilità consultare il capitolo corrispondente della guida.

8.2.1 Nelle finestre di dialogo

Shortcut	Descrizione
Ctrl + Tab Ctrl + Page down	Navigazione in Control Center Passa alla rubrica successiva.
Ctrl + Shift + Tab Ctrl + Page up	Navigazione in Control Center Passa alla rubrica precedente.
← ↑ → ↓	Navigazione nelle rubriche di configurazione Evidenzia con il mouse una rubrica di configurazione.
Tab	Passa all'opzione successiva o al successivo gruppo di opzioni.
Shift + Tab	Passa all'opzione precedente o al precedente gruppo di opzioni.
← ↑ → ↓	Effettua una modifica tra le opzioni di un menu a tendina selezionate o tra più opzioni in un gruppo di opzioni.
Barra spaziatrice	Attiva o disattiva una casella di controllo se l'opzione attiva è una casella di controllo.
Alt + lettera sottolineata	Seleziona l'opzione o esegui il comando.
Alt + ↓ F4	Apri il menu a tendina selezionato.
Esc	Chiudi il menu a tendina selezionato. Annulla il comando e chiudi la finestra di dialogo.
Invio	Esegui comando per l'opzione o il pulsante attivo.

8.2.2 Nella Guida in linea

Shortcut	Descrizione
Alt + barra spaziatrice	Visualizza il menu del sistema.
Alt + Tab	Passa dalla Guida in linea ad altre finestre aperte.
Alt + F4	Chiudi la Guida in linea.
Shift+ F10	Visualizza menu contestuali della Guida in linea.
Ctrl + Tab	Passa alla rubrica successiva nella finestra di navigazione.
Ctrl + Shift + Tab	Passa alla rubrica precedente nella finestra di navigazione.
Page up	Passa all'argomento che è visualizzato sopra l'argomento attuale nel

	sommario, nell'indice o nell'elenco dei risultati della ricerca.
Page down	Passa all'argomento che è visualizzato sotto l'argomento attuale nel sommario, nell'indice o nell'elenco dei risultati della ricerca.
Page up Page down	Sfoglia le voci su un argomento.

8.2.3 In Control Center

Generale

Shortcut	Descrizione
F1	Visualizza Guida in linea
Alt + F4	Chiudi Control Center
F5	Aggiorna visualizzazione
F8	Apri configurazione
F9	Avvia aggiornamento

Rubrica Scansiona

Shortcut	Descrizione
F3	Avvia la scansione con il profilo selezionato
F4	Crea collegamento sul desktop per il profilo selezionato

Rubrica Quarantena

Shortcut	Descrizione
F2	Scansiona nuovamente l'oggetto
F3	Ripristina l'oggetto
F4	Invia l'oggetto
F6	Ripristina l'oggetto in...
Invio	Proprietà
Agg	Aggiungi file
Canc	Elimina l'oggetto

Rubrica Scheduler

Shortcut	Descrizione
F2	Modifica job

Invio	Proprietà
Agg	Inserisci nuovo job
Canc	Elimina job

Rubrica Report

Shortcut	Descrizione
F3	Visualizza il file di report
F4	Stampa il file di report
Invio	Mostra il report
Canc	Elimina report

Rubrica Eventi

Shortcut	Descrizione
F3	Esporta evento
Invio	Mostra evento
Canc	Elimina evento

8.3 Centro sicurezza di Windows

- a partire da Windows XP Service Pack 2 -

8.3.1 Generale

Il Centro sicurezza di Windows verifica lo stato di un computer dal punto di vista della sicurezza.

Se viene rilevato un problema in uno di questi punti importanti (ad esempio un programma antivirus vecchio), il Centro sicurezza invia un avviso e fornisce dei suggerimenti per proteggere più efficacemente il computer.

8.3.2 Il Centro sicurezza di Windows e Avira AntiVir Personal

Software di protezione antivirus/Protezione da software dannoso

È possibile ricevere i seguenti avvisi dal Centro sicurezza di Windows in relazione alla protezione antivirus.

Protezione antivirus NON TROVATA

Protezione antivirus NON AGGIORNATA

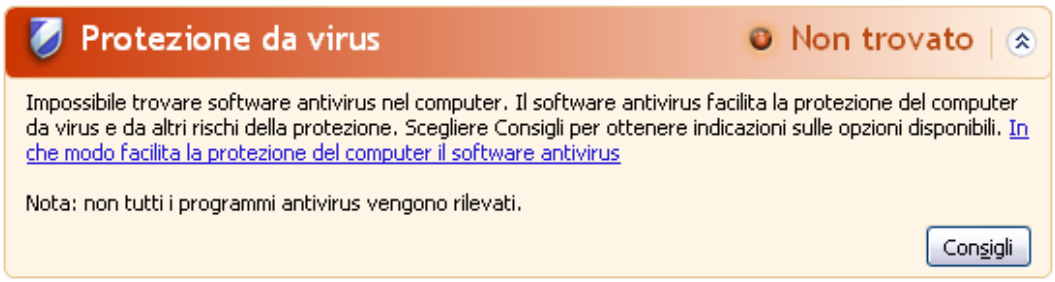
Protezione antivirus ATTIVA

Protezione antivirus INATTIVA

Protezione antivirus NON MONITORATA

Protezione antivirus NON TROVATA

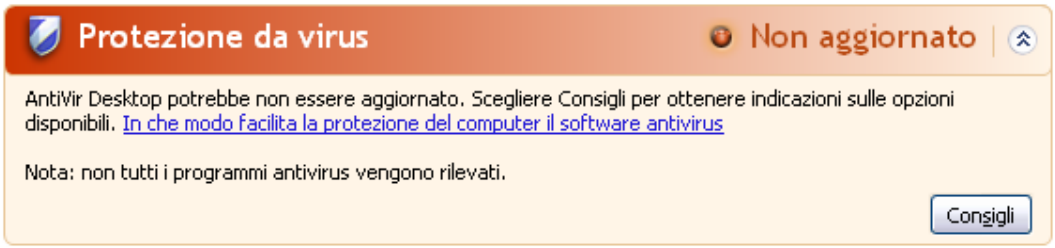
Questo avviso del Centro sicurezza di Windows viene visualizzato quando quest'ultimo non ha rilevato alcun software antivirus sul computer.


Protezione da virus
Non trovato
Impossibile trovare software antivirus nel computer. Il software antivirus facilita la protezione del computer da virus e da altri rischi della protezione. Scegliere Consigli per ottenere indicazioni sulle opzioni disponibili. In che modo facilita la protezione del computer il software antivirus
Nota: non tutti i programmi antivirus vengono rilevati.
Consigli

Nota
Installare Avira AntiVir Personal sul computer per proteggerlo da virus e altri programmi indesiderati!

Protezione antivirus NON AGGIORNATA

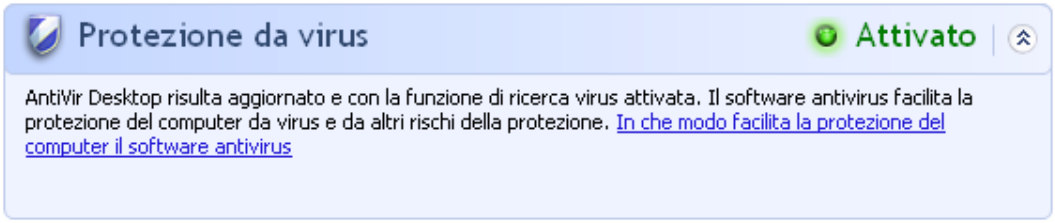
Se si possiede Windows XP Service Pack 2 o Windows Vista e si installa successivamente Avira AntiVir Personal oppure si installa Windows XP Service Pack 2 o Windows Vista su un sistema su cui è già installato Avira AntiVir Personal, si riceve il seguente messaggio:


Protezione da virus
Non aggiornato
AntiVir Desktop potrebbe non essere aggiornato. Scegliere Consigli per ottenere indicazioni sulle opzioni disponibili. In che modo facilita la protezione del computer il software antivirus
Nota: non tutti i programmi antivirus vengono rilevati.
Consigli

Nota
Per far sì che il Centro sicurezza di Windows riconosca Avira AntiVir Personal come aggiornato, dopo l'installazione è necessario eseguire un aggiornamento. Aggiornare il sistema eseguendo un Avira AntiVir Personalaggiornamento.

Protezione antivirus ATTIVA

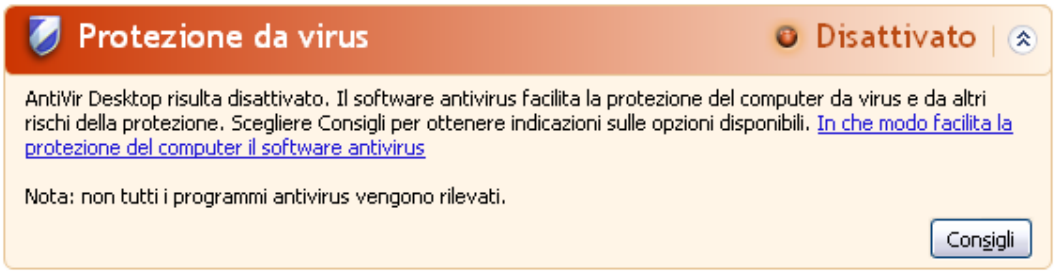
Dopo l'installazione di Avira AntiVir Personal e un susseguente aggiornamento si riceve la seguente nota:


Protezione da virus
Attivato
AntiVir Desktop risulta aggiornato e con la funzione di ricerca virus attivata. Il software antivirus facilita la protezione del computer da virus e da altri rischi della protezione. In che modo facilita la protezione del computer il software antivirus

Avira AntiVir Personal è aggiornato e AntiVir Guard è attivo.

Protezione antivirus INATTIVA

Si riceve la seguente nota se si disattiva AntiVir Guard o si arresta il servizio Guard.

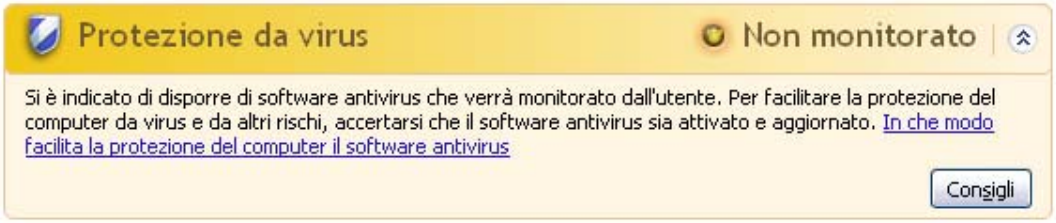

Protezione da virus
Disattivato
AntiVir Desktop risulta disattivato. Il software antivirus facilita la protezione del computer da virus e da altri rischi della protezione. Scegliere Consigli per ottenere indicazioni sulle opzioni disponibili. In che modo facilita la protezione del computer il software antivirus
Nota: non tutti i programmi antivirus vengono rilevati.
Consigli

Note
È possibile attivare e disattivare AntiVir Guard nella rubrica Panoramica :: Stato del Control Center di Avira AntiVir Personal. Inoltre AntiVir Guard viene riconosciuto come attivato quando l'ombrellino rosso nella barra delle applicazioni è aperto.

Protezione antivirus NON MONITORATA

Si riceve il seguente messaggio dal Centro sicurezza di Windows poiché si è optato per l'automonitoraggio del software antivirus.

Nota
La funzione non è supportata da Windows Vista.


Protezione da virus
Non monitorato
Si è indicato di disporre di software antivirus che verrà monitorato dall'utente. Per facilitare la protezione del computer da virus e da altri rischi, accertarsi che il software antivirus sia attivato e aggiornato. In che modo facilita la protezione del computer il software antivirus
Consigli

Nota
Il Centro sicurezza di Windows è supportato da Avira AntiVir Personal. È possibile attivare questa opzione in ogni momento con il pulsante "Consigli...".

Nota
Anche se si possiede Windows XP Service Pack 2 o Windows Vista installati si ha comunque bisogno di una soluzione antivirus, ad esempio Avira AntiVir Personal. Sebbene Windows XP Service Pack 2 controlli il software antivirus non ha alcuna funzione antivirus. L'utente non sarebbe protetto contro virus e malware senza una soluzione antivirus aggiuntiva!

9 Virus e altro

9.1 Categorie estese delle minacce

Programmi di selezione a pagamento (DIALER)

Alcuni servizi offerti in Internet sono a pagamento. In Germania la fatturazione avviene per programmi di selezione con i numeri 0190/0900 (in Austria e Svizzera con i numeri 09x0; in Germania a medio termine passerà ai numeri 09x0). Installati sul computer, questi programmi - in breve dialer - garantiscono la creazione della connessione mediante i numeri Premium-Rate, la cui tariffa può variare enormemente.

La commercializzazione di contenuti online mediante la bolletta telefonica è legale e può essere vantaggiosa per l'utente. I dialer seri non hanno alcun dubbio sul fatto che il cliente sia consapevole e lo utilizzi in modo avveduto. Tali contenuti si installano sul computer dell'utente solo se l'utente dà la propria approvazione, espressa sulla base di un'etichettatura ben riconoscibile o di una richiesta univoca e chiara. La creazione della connessione di programmi dialer seri viene visualizzata in maniera chiara e non ambigua. Inoltre, i dialer seri informano l'utente in maniera esatta e precisa sui costi correlati.

Purtroppo però esistono dialer che si installano senza farsi notare, in maniera dubbia o addirittura fraudolenta. Sostituiscono, ad esempio, la connessione standard dial up dell'utente di Internet all'ISP (Internet-Service-Provider) e a ogni connessione selezionano numeri a pagamento spesso estremamente costosi, come i numeri 0190/0900. L'utente interessato nota dalla bolletta successiva che si è installato un programma dialer indesiderato che si connette a ogni accesso a Internet ai numeri a pagamento 0190/0900 - determinando così una bolletta estremamente cara.

Per proteggersi da programmi di selezione non desiderati e a pagamento (dialer 0190/0900), consigliamo di rivolgersi direttamente al proprio gestore telefonico per bloccare questo tipo di numeri.

Di default, Avira AntiVir Personal riconosce i programmi di selezione a pagamento a lui noti.

Se nella configurazione di Categorie estese delle minacce è stata attivata l'opzione **Programmi di selezione a pagamento (DIALER)** con un segno di spunta, in caso di rilevamento di un programma di selezione a pagamento viene emesso un messaggio di avviso. Si ha quindi la possibilità di eliminare facilmente gli eventuali dialer indesiderati per i numeri 0190/0900. Se si tratta di un programma di selezione a pagamento voluto, si può dichiarare un file da escludere che non verrà più scansionato in futuro.

Giochi (GAMES)

I giochi per computer devono esistere, ma non necessariamente sul luogo di lavoro (ad eccezione a volte della pausa pranzo). Tuttavia i dipendenti delle aziende e i collaboratori degli enti pubblici spesso usano i giochi. Su Internet sono disponibili moltissimi giochi. Anche i giochi per email stanno conoscendo una rapida espansione: dai semplici scacchi fino alla "battaglia navale" numerose sono le varianti in circolazione: i giochi vengono inviati per email ai partner e accettati da questi ultimi.

Alcune ricerche hanno dimostrato che il tempo durante l'orario lavorativo dedicato ai giochi per computer sta assumendo proporzioni rilevanti. Pertanto è comprensibile che sempre più aziende prendano in considerazione la possibilità di eliminare i giochi dai computer utilizzati per lavoro.

Avira AntiVir Personal riconosce i giochi per computer. Se nella configurazione in Categorie estese delle minacce l'opzione **Giochi (GAMES)** è attivata con un segno di spunta, si riceve un avviso se Avira AntiVir Personal ha eseguito un rilevamento. Il gioco è finito nel vero senso della parola visto che è possibile escluderlo facilmente.

Programmi ludici (JOKES)

I programmi ludici possono inorridire qualcuno o divertire tutti, senza essere dannosi o moltiplicarsi. La maggior parte delle volte il computer dopo il richiamo del programma ludico inizia a far suonare una melodia o a visualizzare qualcosa di insolito sullo schermo. Esempi di programmi ludici sono le lavatrici nel drive del floppy disk (DRAIN.COM) o il divoraschermo (BUGSRES.COM).

Ma attenzione! Tutte le manifestazioni di un programma ludico potrebbero anche essere prodotte da un virus o un trojan. L'effetto minimo sull'utente è uno spavento ma si può anche andare nel panico per la paura dei danni che possono verificarsi.

Avira AntiVir Personal è in grado di riconoscere i programmi ludici mediante un'estensione delle proprie routine di scansione ed eventualmente di eliminare il programma indesiderato. Se nella configurazione in Categorie estese delle minacce è stata selezionata l'opzione **Programmi ludici (JOKES)** con un segno di spunta si viene informati sui relativi rilevamenti.

Security Privacy Risk (SPR)

Software che minano la sicurezza del sistema, causano funzioni di programma non desiderate, violano la sfera privata o spiano il comportamento dell'utente e che sono quindi generalmente indesiderati.

Avira AntiVir Personal riconosce il software "Security Privacy Risk". Se nella configurazione in Categorie estese delle minacce è stata attivata l'opzione **Security Privacy Risk (SPR)** con un segno di spunta, si riceve un avviso quando Avira AntiVir Personal effettua un rilevamento.

Software di gestione backdoor (BDC)

Per prelevare dati o manipolare il sistema viene inserito "dalla porta posteriore" un programma server backdoor senza che l'utente se ne accorga. Questo programma può essere gestito da terzi mediante Internet o la rete con un software di gestione backdoor (Client).

Avira AntiVir Personal riconosce "Software di gestione backdoor". Se nella configurazione in Categorie estese delle minacce l'opzione **Software di gestione backdoor (BDC)** è attivata con un segno di spunta, si riceve un avviso quando Avira AntiVir Personal esegue un rilevamento.

Adware/Spyware (ADSPY)

Software che visualizza messaggi pubblicitari o che invia i dati personali dell'utente, spesso a sua insaputa, a terzi e che risulta quindi indesiderato.

Avira AntiVir Personal riconosce gli "Adware/Spyware". Se nella configurazione in Categorie estese delle minacce l'opzione **Adware/Spyware (ADSPY)** è attivata con un segno di spunta, si riceve un avviso quando Avira AntiVir Personal esegue un rilevamento.

Programmi zip runtime insoliti (PCK)

I file compressi con un programma zip runtime insolito possono essere identificati come sospetti.

Avira AntiVir Personal riconosce i "Programmi zip runtime insoliti". Se nella configurazione in Categorie estese delle minacce l'opzione **Programmi zip runtime insoliti (PCK)** è attivata con un segno di spunta, si riceve un avviso quando Avira AntiVir Personal effettua un rilevamento.

File con estensioni occultate (HEUR-DBLEXT)

File eseguibili che occultano la propria estensione in modo sospetto. Il metodo dell'occultamento viene spesso utilizzato dai malware.

Avira AntiVir Personal riconosce i "file con estensioni occultate". Se nella configurazione in Categorie estese delle minacce l'opzione **File con estensioni occultate (HEUR-DBLEXT)** è attivata con un segno di spunta, si riceve un avviso quando Avira AntiVir Personal effettua un rilevamento.

Phishing

Il phishing, anche noto come *brand spoofing* è una forma raffinata di furto dei dati per i clienti o i potenziali clienti di provider Internet, banche, servizi di banking online, enti di registrazione.
Con la trasmissione dell'indirizzo email in Internet, la compilazione di moduli online, la partecipazione a newsgroup o siti Web è possibile che vengano sottratti i dati dai cosiddetti "Internet crawling spiders" e utilizzati senza autorizzazione per frodi o altre attività illegali.

Avira AntiVir Personal riconosce il "Phishing". Se nella configurazione in Categorie estese delle minacce l'opzione **Phishing** è attivata con un segno di spunta, si riceve un avviso quando Avira AntiVir Personal effettua un rilevamento.

Applicazione (APPL)

Con la denominazione APPL si intende un'applicazione il cui utilizzo può essere rischioso o la cui origine è dubbia.

Avira AntiVir Personal riconosce l'"Applicazione (APPL)". Se nella configurazione in Categorie estese delle minacce l'opzione **Applicazione (APPL)** è attivata con un segno di spunta, si riceve un avviso se Avira AntiVir Personal effettua un rilevamento.

9.2 Virus e altri malware

Adware

Con Adware si designa un software che mostra all'utente i banner e i pop up pubblicitari. Questi inserti pubblicitari generalmente non possono essere chiusi e sono quasi sempre visibili. I dati della connessione permettono numerosi feedback sul comportamento dell'utente e sono problematici per motivi di sicurezza dei dati.

Backdoor

Un Backdoor (italiano: porta posteriore) permette, aggirando la tutela all'accesso, di ottenere l'accesso a un computer.

Un programma in esecuzione di nascosto permette a un aggressore di godere di diritti pressoché illimitati. Con l'aiuto del backdoor i dati personali dell'utente possono essere spiati. I backdoor però vengono utilizzati soprattutto per installare altri virus o worm sul sistema infetto.

Virus dei record di avvio

Il record di avvio e il record master di avvio degli hard disk vengono inficiati di preferenza da virus dei record di avvio, che sovrascrivono informazioni importanti all'avvio del sistema. Una delle conseguenze spiacevoli: il sistema operativo non può più essere caricato...

Bot-Net

Per Bot-Net si intende una rete di PC gestibile a distanza (in Internet), composta da bot che comunicano l'uno con l'altro. Questo controllo si raggiunge con virus e trojan che inficiano il computer e poi aspettano indicazioni senza apportare danni al computer intaccato. Queste reti possono essere utilizzare per la diffusione di spam, attacchi DDoS, ecc., talvolta senza che gli utenti del PC si accorgano di alcunché. Il potenziale principale dei Bot-Net è quello di poter raggiungere reti di migliaia di computer, la cui portata salta gli accessi a Internet.

Exploit

Un Exploit (lacuna di sicurezza) è un programma del computer o uno script che sfrutta le debolezze specifiche o le funzioni errate di un sistema operativo o del programma. Una forma di Exploit sono gli attacchi da Internet con l'aiuto di pacchetti di dati manipolati, che sfruttano le debolezze nel software di rete. Con l'utilizzo di alcuni programmi che si introducono clandestinamente si ottiene un più ampio accesso.

hoax (scherzo, burla)

Da un paio di anni gli utenti ricevono avvisi di virus che potrebbero diffondersi per email in Internet o in altre reti. Questi avvisi vengono distribuiti per email con la richiesta di inoltrarli a quanti più colleghi e utenti possibili per mettere in guardia sul "pericolo".

Honeypot

Un Honeypot (pentola di miele) è un servizio installato in una rete (programma o server). Esso ha il compito di monitorare una rete e registrare gli attacchi. Questo servizio è sconosciuto all'utente legittimo e quindi non viene mai toccato. Quando un aggressore cerca punti di debolezza in una rete e prende in considerazione i servizi offerti da un Honeypot viene registrato e viene emesso un allarme.

Macrovirus

I macrovirus sono piccoli programmi che sono scritti nella lingua delle macro di un'applicazione (ad esempio WordBasic in WinWord 6.0) e normalmente potrebbero diffondersi all'interno di documenti di questa applicazione. Essi vengono pertanto chiamati anche virus dei documenti. Per renderli attivi è necessario avviare l'applicazione corrispondente ed eseguire una delle macro infette. Diversamente dai virus "normali" i macrovirus non riguardano file eseguibili ma documenti dell'applicazione host.

Pharming

Il pharming è una manipolazione del file host dei browser Web, per reindirizzare richieste dei siti Web falsificati. Si tratta di una rielaborazione del classico phishing. I truffatori che si servono del pharming godono di grandi quantità di server sui quali vengono archiviati i siti Web falsificati. Il pharming si è consolidato come iperonimo per diversi tipi di attacchi al DNS. In caso di manipolazione del file host con l'ausilio di un trojan o un virus viene effettuata una manipolazione del sistema. La conseguenza è che sono richiamabili solo siti Web falsificati da questo sistema, se l'indirizzo Web viene inserito correttamente.

Phishing

Phishing significa letteralmente pescare dati personali degli utenti di Internet. Il phisher invia generalmente alla vittima lettere aventi valore ufficiale, come ad esempio email che veicolano informazioni sensibili, soprattutto nomi utenti e password o PIN e TAN di accessi all'Online-Banking, approfittando della sua buona fede. Con i dati di accesso rubati il phisher assume l'identità della vittima e conduce operazioni a suo nome. Una cosa è certa: le banche e le assicurazioni non chiedono mai di inviare numeri di carte di credito, PIN, TAN o altri dati di accesso per email, SMS o telefonicamente.

Virus polimorfi

I veri campioni del mimetismo e del travestimento sono i virus polimorfi. Modificano i codici di programmazione e sono pertanto difficili da riconoscere.

Virus di programma

Un virus del computer è un programma che ha la capacità, una volta richiamato, di agganciarsi in qualche modo ad altri programmi e, da tale posizione, di inficiare il sistema. I virus si diffondono quindi in contrasto alle bombe logiche e ai trojan stessi. Al contrario di un worm, un virus ha bisogno di un programma estraneo ospite in cui archiviare il proprio codice virulento. Normalmente, la funzionalità del programma ospite non viene modificata.

Rootkit

Un Rootkit è un insieme di strumenti software che vengono installati su un computer dopo un'irruzione per nascondere il login dell'intruso, nascondere processi e registrare dati, in linea generale: per rendersi invisibile. I rootkit tentano di aggiornare i programmi spia già installati e di installare nuovamente gli spyware eliminati.

Virus di script e worm

Questi virus sono estremamente semplici da programmare e in poche ore si diffondono per email a livello globale, premesso che siano presenti tecniche ad hoc.

I virus di script e i worm utilizzano la lingua degli script, come ad esempio Javascript, VBScript ecc., per inserirsi in altri nuovi script o per diffondersi mediante il richiamo di funzioni del sistema operativo. Spesso ciò avviene tramite email o mediante lo scambio di file (documenti).

Il worm è un programma che non intacca alcun documento ospite. I worm non possono quindi divenire una componente di altri programmi. I worm rappresentano spesso l'unica possibilità di introdursi clandestinamente su sistemi dotati di provvedimenti restrittivi legati alla sicurezza.

Spyware

Gli spyware sono i cosiddetti programmi spia che inviano dati personali dell'utente a terzi senza che questi ne siano a conoscenza e senza l'approvazione del produttore del software. I programmi spyware servono soprattutto ad analizzare la navigazione in Internet e a introdurre banner o pop up pubblicitari in maniera mirata.

Cavalli di Troia (in breve trojan)

I trojan sono sempre più diffusi. Così vengono definiti i programmi che pretendono di avere una funzione precisa; dopo il loro avvio, tuttavia, mostrano il loro vero volto ed eseguono altre funzioni che hanno per lo più effetti distruttivi. I trojan non possono moltiplicarsi da soli e in questo si differenziano dai virus e dai worm. La maggior parte di loro ha un nome interessante (SEX.EXE o STARTME.EXE), che ha la funzione di spingere l'utente a eseguire il trojan. Subito dopo l'esecuzione diventano attivi e formattano, ad esempio, l'hard disk. Un tipo particolare di trojan è il dropper, che "lascia cadere" i virus, ovvero li installa nel sistema del computer.

Zombie

Un PC zombie è un calcolatore che è intaccato da programmi malware e permette all'hacker di abusare del computer mediante la gestione a distanza per fini criminali. Il PC infetto lancia il comando, ad esempio, di attacchi di Denial-of-Service- (DoS) o invia spam o email di phishing.

10 Info e Service

In questo capitolo si ottengono informazioni sui modi in cui è possibile tenersi in contatto con noi.

vedere capitolo Indirizzo di contatto

vedere capitolo Supporto tecnico

vedere capitolo File sospetto

vedere capitolo Comunicare un falso allarme

10.1 Indirizzi di contatto

Siamo a disposizione del cliente qualora avesse domande o suggerimenti sul mondo dei prodotti di Avira AntiVir Personal. I nostri indirizzi dove contattarci sono disponibili in Guida in linea :: Su Avira AntiVir Personal.

10.2 Supporto tecnico

Il supporto Avira AntiVir Personal è rivolto all'utente, serve a rispondere alle sue domande o a risolvere un problema tecnico.

Sul nostro sito Web http://www.avira.it/personal-support l'utente può riferire tutte le informazioni utili per il nostro ampio servizio di supporto.

Per poter ricevere aiuto nel modo migliore e più veloce possibile l'utente deve prendere in considerazione le seguenti informazioni:

- **Informazioni sulla versione**. Essi si trovano sull'interfaccia del programma nella voce di menu Guida in linea :: Informazioni su AntiVir Personal :: Informazioni sulla versione.
- **Versione del sistema operativo** e service pack eventualmente installati.
- **I pacchetti software installati**, ad esempio software antivirus di altri produttori.
- **Messaggi precisi** del programma o del file di report.

10.3 File sospetto

I virus che non possono essere riconosciuti o eliminati dai nostri prodotti così come i file sospetti possono essere inviati a noi. A tale scopo sono disponibili diverse modalità di invio.

- Selezionare il file nel Gestore della quarantena di Control Center e selezionare la voce Invia file mediante il menu contestuale o i pulsanti corrispondenti.

– Allegare il file desiderato compresso (WinZIP, PKZip, Arj, ecc.) ad un'email e inviarlo a virus-personal@avira.it. Poiché alcuni Email-Gateways operano con software antivirus, si prega di proteggere il file/i file con una password (non dimenticare di comunicare anche la password).

10.4 Comunicare un falso allarme

Se si ritiene che Avira AntiVir Personal abbia segnalato un rilevamento in un file che tuttavia con tutta probabilità è "pulito", si prega di inviare tale file compresso (WinZIP, PKZIP, Arj, ecc.) per email come allegato a virus-personal@avira.it. Poiché alcuni Email-Gateways operano con software antivirus, si prega di proteggere il file/i file con una password (non dimenticare di comunicare anche la password).

11 Riferimento: Opzioni di configurazione

Il riferimento della configurazione elenca le opzioni di configurazione disponibili in Avira AntiVir Personal.

11.1 Sistema di scansione

La rubrica Sistema di scansione della configurazione è dedicata alla configurazione della scansione diretta, ovvero alla scansione su richiesta.

11.1.1 Scansione

Qui si può definire la procedura standard della routine di scansione durante una scansione diretta. Se si seleziona una determinata directory da controllare durante la scansione diretta, il sistema di scansione esegue i controlli in base alla configurazione:

- con una determinata prestazione di scansione (priorità),
- anche sui record di avvio e nella memoria principale,
- su alcuni o tutti i record di avvio e nella memoria principale,
- su tutti i file o i file selezionati nella directory.

File

Il sistema di scansione può utilizzare un filtro per scansionare solamente i file con una determinata estensione (tipo).

Tutti i file

Se l'opzione è attivata, viene eseguita una ricerca di virus e programmi indesiderati in tutti i file indipendentemente dal contenuto e dall'estensione. Il filtro non viene utilizzato.

Nota
Se Tutti i file è attivo, il pulsante **Estensioni file** non è selezionabile.

Utilizza estensioni smart

Se l'opzione è attivata, la selezione dei file da scansionare viene effettuata automaticamente da Avira AntiVir Personal. Ciò significa che Avira AntiVir Personal decide, in base al contenuto di un file, se quest'ultimo deve essere controllato o meno per verificare la presenza di virus e programmi indesiderati. Questa procedura è lievemente più lenta di Utilizza elenco estensione file, ma molto più sicura poiché i controlli non vengono effettuati solamente sulla base delle estensioni dei file. Questa opzione è attivata di default ed è consigliata.

Nota
Se Utilizza estensioni smart è attivo, il pulsante **Estensioni file** non è selezionabile.

Utilizza elenco estensioni file

Se l'opzione è attivata, vengono scansionati solo i file con una determinata estensione. Sono preimpostati tutti i tipi di file che possono contenere virus e programmi indesiderati. L'elenco può essere modificato manualmente mediante il pulsante **Estensioni file**.

Nota
Se questa opzione è attiva e tutte le voci dell'elenco delle estensioni dei file sono state eliminate, viene visualizzato il testo "Nessuna estensione dei file" sotto il pulsante **Estensioni file** .

Estensioni file

Con questo pulsante viene richiamata una finestra di dialogo nella quale sono riportate tutte le estensioni dei file che vengono controllate durante una scansione in modalità **Utilizza elenco estensioni file**. Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o eliminare voci.

Nota
Prestare attenzione al fatto che l'elenco standard può variare da versione a versione.

Impostazioni aggiuntive

Record di avvio dei drive di scansione

Se l'opzione è attivata, il sistema di scansione controlla i record di avvio dei drive selezionati durante la scansione diretta. Questa opzione è attivata di default.

Scansione dei record master di avvio

Se l'opzione è attivata, il sistema di scansione controlla i record master di avvio degli/dell'hard disk utilizzati/o nel sistema.

Ignora file offline

Se l'opzione è attivata, la scansione diretta ignora completamente i cosiddetti file offline durante la scansione. Ciò significa che in questi file non viene controllata la presenza di virus e programmi indesiderati. I file offline sono i file che sono stati archiviati fisicamente dall'hard disk, ad es. su un nastro, mediante il cosiddetto sistema gerarchico di gestione della memoria (HSM). Questa opzione è attivata di default.

Verifica integrità dei file di sistema

Se l'opzione è attivata, i principali file di sistema di Windows vengono sottoposti a una verifica particolarmente sicura durante ogni scansione diretta per verificare la presenza di modifiche dovute a malware. Se viene individuato un file modificato, questo viene segnalato come rilevamento sospetto. La funzionalità occupa molta memoria. Per questo motivo l'opzione è disattivata di default.

Importante
L'opzione è disponibile solo a partire da Windows Vista.

Nota
Se si utilizzano strumenti di terzi, si modificano i file di sistema o si personalizza la schermata di avvio, questa opzione non deve essere utilizzata. Questi strumenti sono, ad esempio, i cosiddetti skinpack, TuneUp Utilities o Vista Customization.

Scansione ottimizzata

Se l'opzione è attivata, la capacità del processore viene utilizzata in modo ottimale durante la scansione con il sistema di scansione. Per motivi di performance, in caso di scansione ottimale, la funzione di log si verifica al massimo a un livello standard.

Nota
L'opzione è disponibile solo per computer multiprocessore.

Segui collegamenti simbolici

Se l'opzione è attivata, il sistema di scansione esegue una scansione di tutti i collegamenti simbolici nel profilo di ricerca o nelle directory selezionate, allo scopo di scansionare i file collegati alla ricerca di virus e malware. Questa opzione non è supportata in Windows 2000 ed è disattivata di default.

Importante
L'opzione non comprende i collegamenti (shortcut), bensì si riferisce esclusivamente ai link simbolici (generati con mklink.exe) o ai punti di giunzione (generati con junction.exe), presenti in modalità trasparente nel file system.

Scansione Rootkit all'avvio della scansione

Se l'opzione è attivata, il sistema di scansione verifica all'avvio della scansione la presenza di rootkit attivi nella directory di sistema Windows tramite una cosiddetta procedura rapida. Questa procedura non verifica se nel computer vi sono rootkit attivi così dettagliatamente come il profilo di ricerca **Cerca rootkit**, ma è molto più rapida.

Importante
Scansione rootkit in Windows XP 64 Bit non disponibile!

Scansiona registro

Se l'opzione è attivata, viene scansionato il registro alla ricerca di software dannosi.

Processo di scansione

Permetti di arrestare il sistema di scansione

Se l'opzione è attivata, la ricerca di virus o programmi indesiderati può essere arrestata in ogni momento con il pulsante **Arresta** nella finestra di "Luke Filewalker". Se questa impostazione è disattivata, il pulsante **Arresta** nella finestra "Luke Filewalker" è grigio. Pertanto non è possibile terminare prematuramente una scansione! Questa opzione è attivata di default.

Priorità del sistema di scansione

Il sistema di scansione differenzia tre livelli di priorità nella scansione diretta. Si tratta di un sistema efficace solo se sul computer sono in esecuzione più processi contemporaneamente. La scelta si ripercuote anche sulla velocità di scansione.

Livello basso

Il sistema di scansione riceve dal sistema operativo il tempo del processore solo se nessun altro processo necessita di tempo di elaborazione, ovvero finché il sistema di scansione è l'unico programma in esecuzione, la velocità è massima. Nel complesso, in questo modo viene gestito molto bene anche il lavoro con altri programmi: il computer è più veloce se altri programmi sono in esecuzione, mentre il sistema di scansione lavora in background. Questa opzione è attivata di default ed è consigliata.

Livello medio

Il sistema di scansione viene eseguito con priorità normale. Tutti i processi ricevono lo stesso tempo di elaborazione dal sistema operativo. In alcune circostanze il lavoro con altre applicazioni ne risulta compromesso.

Livello elevato

Il sistema di scansione riceve la massima priorità. Un lavoro parallelo con altre applicazioni è pressoché impossibile. Tuttavia il sistema completa la scansione in maniera estremamente rapida.

11.1.1.1. Azione in caso di rilevamento

Azione in caso di rilevamento

È possibile definire azioni che il sistema di scansione deve eseguire quando viene rilevato un virus o un programma indesiderato.

Interattivo

Se l'opzione è attivata, i rilevamenti della scansione del sistema vengono notificati in una finestra di dialogo. Al termine della scansione, si riceve un avviso con l'elenco dei file infetti rilevati. Mediante il menu contestuale è possibile selezionare un'azione da eseguire per i singoli file infetti. È possibile eseguire l'azione selezionata per tutti i file infetti oppure interrompere la scansione.

Nota
Di default nella finestra di dialogo è preselezionata l'azione 'Sposta in quarantena'. È possibile selezionare ulteriori azioni mediante il menu contestuale.

È possibile reperire maggiori informazioni qui.

Automatico

Se l'opzione è attivata, in caso di rilevamento di virus o di programmi indesiderati non appare alcuna finestra di dialogo in cui selezionare l'azione da eseguire. Il sistema di scansione reagisce conformemente alle impostazioni effettuate precedentemente dall'utente in questa sezione.

Copia il file in quarantena prima dell'azione

Se l'opzione è attivata, il sistema di scansione crea una copia di sicurezza (backup) prima dell'esecuzione delle azioni primarie e secondarie desiderate. La copia di sicurezza viene mantenuta in Quarantena dove il file può essere ripristinato se possiede un valore informativo. Inoltre è possibile inviare la copia di sicurezza ad Avira Malware Research Center per ulteriori indagini.

Azione primaria

L'azione primaria è l'azione che viene eseguita quando il sistema di scansione rileva un virus o un programma indesiderato. Se l'opzione **Ripara** è attiva, ma la riparazione del file infetto non è possibile, verrà eseguita l'azione definita in **Azione secondaria**.

Nota
L'opzione **Azione secondaria** è selezionabile solo se in **Azione primaria** è stata selezionata l'impostazione **Ripara**.

ripara

Se l'opzione è attivata, il sistema di scansione ripara automaticamente i file infetti. Se il sistema di scansione non può riparare un file infetto, in alternativa esegue l'opzione selezionata in Azione secondaria.

Nota
Si consiglia una riparazione automatica, che tuttavia comporta una modifica dei file presenti sul computer da parte del sistema di scansione.

elimina

Se l'opzione è attivata, il file viene eliminato.

rinomina

Se l'opzione è attivata, il sistema di scansione rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere successivamente riparati e nuovamente rinominati.

ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

Quarantena

Se l'opzione è attivata, il sistema di scansione sposta il file in quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Azione secondaria

L'opzione **Azione secondaria** è selezionabile solo se in **Azione primaria** è stata selezionata l'impostazione Ripara. Con questa opzione si può decidere come procedere con il file infetto se non è riparabile.

elimina

Se l'opzione è attivata, il file viene eliminato.

rinomina

Se l'opzione è attivata, il sistema di scansione rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

Quarantena

Se l'opzione è attivata, il sistema di scansione sposta il file in quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Nota
Se si seleziona **Elimina** o come azione principale o secondaria, attenersi alle seguenti indicazioni: in caso di rilevamento di oggetti euristici, i file infetti non vengono eliminati, bensì spostati in quarantena.

Per la ricerca negli archivi il sistema di scansione utilizza una scansione ricorsiva: vengono decompressi anche gli archivi in altri archivi e viene controllata la presenza di virus e programmi indesiderati. I file compressi vengono scansionati, decompressi e nuovamente scansionati.

Scansiona archivi

Se l'opzione è attivata, vengono scansionati gli archivi selezionati nell'elenco degli archivi. Questa opzione è attivata di default.

Tutti i tipi di archivio

Se l'opzione è attivata, vengono selezionati e scansionati tutti i tipi di archivi nell'elenco degli archivi.

Smart Extension

Se l'opzione è attivata, il sistema di scansione riconosce se un file è in formato compresso (archivio), anche se l'estensione è diversa da quelle abituali, e scansiona l'archivio. Tuttavia a tal fine ogni file deve essere aperto, riducendo così la velocità della scansione. Esempio: se un archivio *.zip ha estensione *.xyz, il sistema di scansione decomprime anche tale archivio e lo scansiona. Questa opzione è attivata di default.

Nota
Vengono scansionati solo quei tipi di archivio che sono selezionati nell'elenco degli archivi.

Limita la profondità di ricorsione

La decompressione e la scansione di archivi particolarmente ramificati può necessitare di molto tempo e molte risorse del sistema. Se l'opzione è attivata, è possibile limitare la profondità di ricorsione della scansione in archivi multipli a un determinato numero di livelli di compressione (profondità di ricorsione massima). In questo modo è possibile risparmiare tempo e risorse del processore.

Nota
Per individuare un virus o un programma indesiderato all'interno di un archivio, il sistema di scansione deve eseguire la scansione fino al livello di ricorsione nel quale si trova il virus o il programma indesiderato.

Profondità massima di ricorsione

Per poter indicare la profondità massima di ricorsione, l'opzione Limita profondità di ricorsione deve essere attivata.
È possibile inserire direttamente la profondità di ricorsione desiderata oppure modificarla per mezzo dei tasti freccia a destra del campo. I valori consentiti sono compresi tra 1 e 99. Il valore standard e consigliato è 20.

Valori standard

Il pulsante crea i valori predefiniti per la scansione degli archivi.

Elenco archivi

In questa sezione è possibile impostare quali archivi devono essere scansionati dal sistema di scansione. A tal fine è necessario selezionare le voci corrispondenti.

11.1.1.2. Eccezioni

Oggetti file da escludere dalla scansione

L'elenco in questa finestra contiene file e percorsi che non devono essere presi in considerazione dal sistema di scansione durante la ricerca di virus e programmi indesiderati.

Si consiglia di inserire quante meno eccezioni possibili e solo i file che non devono essere scansionati durante una scansione normale per qualsivoglia motivo. Consigliamo di far comunque controllare la presenza di virus o programmi indesiderati in questi file prima di inserirli in questo elenco!

Nota
Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Attenzione
Questi file non vengono presi in considerazione durante la scansione!

Nota
I file inseriti in questo elenco vengono segnalati nel file di report. Controllare di tanto in tanto nel file di report la presenza di questi file non scansionati poiché potrebbe non sussistere più il motivo per il quale sono stati esclusi. In questo caso i nomi di questi file dovrebbero essere eliminati dall'elenco.

Campo

Inserire in questo campo il nome del file che non deve essere preso in considerazione durante una scansione diretta. Di default non è indicato alcun file.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il file o il percorso desiderato.
Se si è fornito un nome di file con un percorso completo, tale file non viene scansionato. Se si è inserito un nome di file senza un percorso, ogni file con tale nome (indipendentemente dal percorso o dal drive) non verrà scansionato.

Aggiungi

Con il pulsante è possibile accettare il file indicato nel campo nella finestra di visualizzazione.

Elimina

Il pulsante elimina una voce selezionata nell'elenco. Questo pulsante non è attivo se non è selezionata alcuna voce.

Nota
Se si aggiunge un'intera partizione all'elenco dei file da escludere, verranno tralasciati dalla scansione solo i file salvati direttamente nella partizione e non i file contenuti in directory all'interno della partizione:
Esempio: file da omettere: `D:\ = D:\file.txt` verrà tralasciato dalla scansione del sistema, invece `D:\folder\file.txt` verrà incluso nella scansione.

11.1.1.3. Euristica

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca di Avira AntiVir Personal.

Avira AntiVir Personal contiene un'euristica molto efficace, che consente di riconoscere in modo proattivo malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche, viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di un malware, potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Macrovirus euristico

Avira AntiVir Personal contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di possibile riparazione vengono eliminate tutte le macro del documento infetto, in alternativa i documenti sospetti vengono solo segnalati e l'utente riceverà un avviso. Questa opzione è attivata di default ed è consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Avira AntiVir Personal contiene, grazie alla tecnologia AntiVir AHeAD, un'euristica molto efficace, in grado di riconoscere anche malware sconosciuti (nuovi). Se l'opzione è attivata è possibile impostare il grado di "rigidità" dell'euristica. Questa opzione è attivata di default.

Livello di riconoscimento basso

Se l'opzione è attivata, Avira AntiVir Personal riconosce un numero inferiore di malware sconosciuti, il rischio di falsi allarmi è limitato.

Livello di riconoscimento medio

Questa opzione è attivata di default, se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, Avira AntiVir Personal riconosce un numero maggiore di malware sconosciuti, ma possono verificarsi messaggi di errore.

11.1.2 Report

Il sistema di scansione possiede una funzione di log molto ampia. In questo modo si ricevono informazioni esatte sui risultati di una scansione diretta. Il file di report contiene tutte le voci del sistema e gli avvisi e i messaggi della scansione diretta.

Nota
Per comprendere quali azioni il sistema di scansione ha eseguito in caso di rilevamento di virus o programmi indesiderati, deve sempre essere creato un file di report.

Funzione di log

Disabilitato

Se l'opzione è attivata, il sistema di scansione non riporta le azioni e i risultati della scansione diretta.

Standard

Se l'opzione è attivata, il sistema di scansione riporta il nome dei file infetti con il percorso. Nel file di report vengono riportate inoltre la configurazione per la scansione attuale, le informazioni sulla versione e sul Licenziatario.

Avanzato

Se l'opzione è attivata, il sistema di scansione riporta anche gli avvisi e le note, oltre alle informazioni standard.

Completo

Se l'opzione è attivata, il sistema di scansione riporta tutti i file scansionati. Inoltre, tutti i file infetti, nonché gli avvisi e le note, vengono registrati nel file di report.

Nota
Se l'utente deve inviare un file di report ad Avira (per la ricerca dell'errore), preghiamo di creare il file di report con questa modalità.

11.2 Guard

La rubrica Guard della configurazione è dedicata alla configurazione della scansione in tempo reale.

11.2.1 Scansione

Solitamente si desidera che il proprio sistema sia costantemente monitorato. Per questo viene utilizzato il Guard (scansione in tempo reale = On-Access Scanner). In questo modo è possibile ricercare la presenza di virus e programmi indesiderati in tutti i file che vengono aperti o copiati sul computer, "on the fly".

Modalità di scansione

Qui si stabilisce il momento in cui effettuare la scansione di un file.

Scansione in lettura

Se l'opzione è attivata, il Guard scansiona i file prima che vengano letti o eseguiti da un'applicazione o dal sistema operativo.

Scansione in scrittura

Se l'opzione è attivata, il Guard scansiona un file in scrittura. Solo al termine di questa procedura è possibile accedere nuovamente al file.

Scansione in lettura e scrittura

Se l'opzione è attivata, il Guard scansiona i file prima dell'apertura, della lettura e dell'esecuzione e dopo la scrittura. Questa opzione è attivata di default ed è consigliata.

File

Il Guard può utilizzare un filtro per scansionare solo i file con una determinata estensione (tipo).

Tutti i file

Se l'opzione è attivata, viene eseguita una ricerca di virus e programmi indesiderati in tutti i file, indipendentemente dal contenuto e dall'estensione.

Nota
Se Tutti i file è attivo, il pulsante **Estensioni file** non è selezionabile.

Utilizza estensioni smart

Se l'opzione è attivata, la selezione dei file da scansionare viene effettuata automaticamente da Avira AntiVir Personal. Ciò significa che Avira AntiVir Personal decide in base al contenuto se un file deve essere controllato o meno per la presenza di virus e programmi indesiderati. Questa procedura è lievemente più lenta di Utilizza elenco estensione file, ma molto più sicura poiché i controlli non vengono effettuati solamente sulla base delle estensioni dei file.

Nota
Se Utilizza estensioni smart è attivo, il pulsante **Estensioni file** non è selezionabile.

Utilizza elenco estensioni file

Se l'opzione è attivata, vengono scansionati solo i file con una determinata estensione. Sono preimpostati tutti i tipi di file che possono contenere virus e programmi indesiderati. L'elenco può essere modificato manualmente mediante il pulsante **Estensioni file**. Questa opzione è attivata di default ed è consigliata.

Nota
Se questa opzione è attiva e tutte le voci dell'elenco delle estensioni dei file sono state eliminate, viene visualizzato il testo "Nessuna estensione dei file" sotto il pulsante **Estensioni file** .

Estensioni file

Con questo pulsante viene richiamata una finestra di dialogo nella quale sono riportate tutte le estensioni dei file che vengono controllate durante una scansione in modalità **Utilizza elenco estensioni file**. Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o eliminare voci.

Nota
Prestare attenzione al fatto che l'elenco estensioni dei file può variare da versione a versione.

Archivi

Scansiona archivi

Se l'opzione è attivata, vengono scansionati gli archivi. I file compressi vengono scansionati, decompressi e nuovamente scansionati. Questa opzione è disattivata di default. La scansione degli archivi viene limitata dalla profondità di ricorsione, dal numero di file da scansionare e dalle dimensioni dell'archivio. È possibile impostare la profondità di ricorsione massima, il numero di file da scansionare e le dimensioni massime dell'archivio.

Nota
L'opzione è disattivata di default poiché il processo occupa molta memoria. Generalmente si consiglia di scansionare gli archivi con la scansione diretta.

Profondità massima di ricorsione

Per la ricerca negli archivi il Guard utilizza una scansione ricorsiva: vengono decompressi anche gli archivi in altri archivi e viene controllata la presenza di virus e programmi indesiderati. L'utente può stabilire la profondità di ricorsione. Il valore standard per la profondità di ricorsione è 1 ed è quello consigliato: tutti gli archivi che si trovano direttamente nell'archivio principale vengono decompressi e scansionati.

Numero massimo dei file

Per la ricerca negli archivi la scansione viene limitata a un numero massimo di file dell'archivio. Il valore standard per il numero massimo di file da scansionare è 10 ed è quello consigliato.

Dimensione massima (KB)

Per la ricerca negli archivi la scansione viene limitata a una dimensione massima degli archivi da decomprimere. Il valore standard è 1000 KB ed è quello consigliato.

11.2.1.1. Azione in caso di rilevamento

Notifiche

Utilizza log eventi

Se l'opzione è attivata viene inserita una voce nel log eventi a ogni rilevamento. L'amministratore può riconoscere i rilevamenti e reagire di conseguenza. Questa opzione è attivata di default.

Avvio automatico

Blocca avvio automatico

Se l'opzione è attivata, l'avvio automatico di Windows viene bloccato su tutti i drive collegati, come penne USB, CD e DVD, drive di rete. Con la funzione di avvio automatico di Windows, i file sui supporti informatici o sui drive di rete vengono letti immediatamente al momento dell'inserimento o del collegamento; in questo modo i file possono essere avviati e riprodotti automaticamente. Tuttavia questa funzionalità nasconde un rischio per la sicurezza molto elevato, poiché con l'avvio automatico dei file è possibile che vengano installati malware e programmi indesiderati. Particolarmente critica è la funzione di avvio automatico delle penne USB poiché su questi supporti i file possono modificarsi continuamente.

Escludi CD e DVD

Se l'opzione è attivata, è consentita la funzione di avvio automatico sui drive CD e DVD.

Attenzione
Disattivare la funzione di avvio automatico per i drive CD e DVD solo se si è sicuri che si tratti di supporti informatici assolutamente affidabili.

11.2.1.2. Eccezioni

Con queste opzioni è possibile configurare gli oggetti soggetti a eccezioni per il Guard (scansione in tempo reale). Gli oggetti identificati verranno così esclusi dalla scansione in tempo reale. Il Guard può ignorare gli accessi ai file riportati nell'elenco dei processi da tralasciare durante la scansione in tempo reale. Questa funzione è utile ad esempio per le banche dati o le soluzioni di backup.

Processi da omettere per il Guard

Tutti gli accessi ai file dei processi indicati in questo elenco sono stati esclusi dal monitoraggio mediante il Guard.

Campo

Inserire in questo campo il nome del processo che deve essere ignorato dalla scansione in tempo reale. Di default non è indicato alcun processo.

Nota
È possibile inserire fino a 128 processi.

Nota
Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Attenzione:
Il percorso indicato e il nome del file del processo non possono superare i 255 caratteri.

Attenzione
Prestare attenzione al fatto che tutti gli accessi ai file dei processi che sono stati evidenziati nell'elenco sono esclusi dalla scansione di virus e programmi indesiderati! Esplora risorse di Windows e il sistema operativo non possono essere esclusi. La voce corrispondente nell'elenco viene ignorata.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare un file eseguibile.

Processi

Il pulsante **Processi** apre la finestra *Selezione del processo*, in cui vengono indicati i processi in corso.

Aggiungi

Con il pulsante è possibile accettare il processo indicato nel campo nella finestra di visualizzazione.

Elimina

Con il pulsante si elimina un processo selezionato dalla finestra di dialogo.

Oggetti file da omettere per il Guard

Tutti gli accessi ai file degli oggetti indicati in questo elenco sono esclusi dal monitoraggio mediante il Guard.

Campo

Inserire in questo campo il nome del file che deve essere ignorato dalla scansione in tempo reale. Di default non è indicato alcun file.

Nota
Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Nota
Per ogni drive è possibile indicare al massimo 20 eccezioni con il percorso completo (che inizia con la lettera del drive).
Ad es.: C:\Programmi\Applicazioni\Nome.log

Il numero massimo di eccezioni senza percorso completo è 64.
Ad es.: *.log

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare i file da escludere.

Aggiungi

Con il pulsante è possibile accettare il file indicato nel campo nella finestra di visualizzazione.

Elimina

Con il pulsante si elimina un oggetto file selezionato dalla finestra di visualizzazione.

Prestare attenzione ai seguenti punti:

- Le wildcard * (molti caratteri) e ? (un solo carattere) sono consentite solo nei nomi del file.
- I nomi delle directory devono concludersi con una barra inversa \, altrimenti viene confuso con un nome di file.
- L'elenco viene elaborato dall'alto verso il basso.
- È possibile anche escludere singole estensioni di file (incluse le wildcard).
- Se una directory viene esclusa, anche tutte le sottodirectory che contiene vengono escluse automaticamente.
- Più lungo è l'elenco, maggiore è il tempo di cui il processore ha bisogno per elaborare l'elenco a ogni accesso. Si consiglia pertanto di mantenere l'elenco più breve possibile.
- Per escludere oggetti anche quando vi si accede con nomi di file DOS brevi (convenzione dei nomi di DOS 8.3), è necessario inserire nell'elenco il nome breve del file corrispondente.

Nota
Un nome di file che contiene wildcard non deve concludersi con una barra inversa.

Ad esempio:

```
C:\Programmi\Applicazioni\applic*.exe\
```

Questa voce non è valida e non viene considerata come un'eccezione!

Nota
In caso di drive dinamici, collegati (montati) come directory a un altro drive, è necessario utilizzare nell'elenco delle eccezioni il nome dell'alias del sistema operativo per il drive collegato:
ad es. \Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
Anche utilizzando il punto di montaggio stesso (mount point), ad es. C:\DynDrive, si esegue comunque la scansione del drive dinamico. È possibile ricavare i nomi dell'alias del sistema operativo da utilizzare dal file di report del Guard.

Nota
In base al file di report del Guard è possibile ricavare i percorsi utilizzati dal Guard durante la ricerca dei file infetti. Nell'elenco delle eccezioni, utilizzare di massima gli stessi percorsi. Procedere come segue: impostare la funzione di log del Guard nella configurazione in Guard :: Report su **Completo**. Quindi accedere con il Guard attivato a file, directory, drive collegati . È ora possibile leggere il percorso da utilizzare dal file di report del Guard. È possibile richiamare il file di report nel Control Center in Protezione locale :: Guard.

Esempi:

```
C:
C:\
C:\*.*
C:\*
*.exe
*.xl?
*.*
C:\Programmi\Applicazioni\applicazione.exe
C:\Programmi\Applicazioni\applicaz*.exe
C:\Programmi\Applicazioni\applicaz*
C:\Programmi\Applicazioni\applicaz????.e*
C:\Programmi\
C:\Programmi
C:\Programmi\Applicazioni\*.mdb
```

11.2.1.3. Euristica

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca di Avira AntiVir Personal.

Avira AntiVir Personal contiene un'euristica molto efficace, che consente di riconoscere in modo proattivo malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche, viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di un malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Macrovirus euristico

Avira AntiVir Personal contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di possibile riparazione vengono eliminate tutte le macro del documento infetto, in alternativa i documenti sospetti vengono solo segnalati e l'utente riceverà un avviso. Questa opzione è attivata di default ed è consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Avira AntiVir Personal contiene, grazie alla tecnologia AntiVir AHeAD, un'euristica molto efficace, in grado di riconoscere anche malware sconosciuti (nuovi). Se l'opzione è attivata è possibile impostare il grado di "rigidità" dell'euristica. Questa opzione è attivata di default.

Livello di riconoscimento basso

Se l'opzione è attivata, Avira AntiVir Personal riconosce un numero inferiore di malware sconosciuti, il rischio di falsi allarmi è limitato.

Livello di riconoscimento medio

Questa opzione è attivata di default se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, Avira AntiVir Personal riconosce un maggior numero di malware sconosciuti, ma possono verificarsi anche messaggi di errore.

11.2.2 Report

Guard possiede una funzione di log molto vasta che può fornire all'utente o all'amministratore informazioni esatte sulla modalità di un rilevamento.

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, il Guard non crea alcun protocollo.
In casi eccezionali si può rinunciare alla funzione di log, ad esempio solo se si eseguono test con molti virus o programmi indesiderati.

Standard

Se l'opzione è attivata, il Guard registra informazioni importanti (su rilevamenti, avvisi ed errori) nel file di report, mentre le informazioni meno importanti vengono ignorate per maggiore chiarezza. Questa opzione è attivata di default.

Avanzato

Se l'opzione è attivata, il Guard registra nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, il Guard registra tutte le informazioni - anche quelle relative alla dimensione del file, al tipo, alla data, ecc. - nel file di report.

Limitazioni del file di report

Limita la dimensione a n MB

Se l'opzione è attivata, il file di report può essere limitato a una determinata dimensione; valori possibili: da 1 a 100 MB. Con la limitazione del file di report si introduce un intervallo di circa 50 kilobyte per non sovraccaricare il processore. Se la dimensione del file di report supera la dimensione indicata di 50 kilobyte, vengono automaticamente eliminate le voci meno recenti fin quando si raggiunge una dimensione inferiore a 50 kilobyte.

Backup file report prima della limitazione

Se l'opzione è attivata, viene eseguito un backup del file di report prima della limitazione.

Scrivi la configurazione nel file di report

Se l'opzione è attivata, la configurazione utilizzata della scansione in tempo reale viene riportata nel file di report.

11.3 Aggiornamento

Nella rubrica *Aggiornamento* configurare l'esecuzione automatica degli aggiornamenti. È possibile impostare diversi intervalli di aggiornamento, nonché attivare o disattivare l'aggiornamento automatico.

Aggiornamento automatico

Attiva

Se l'opzione è attivata, gli aggiornamenti automatici vengono eseguiti nell'intervallo di tempo indicato, nonché al verificarsi degli eventi attivati.

Aggiornamento automatico ogni n giorni / ore / minuti

In questo campo è possibile indicare l'intervallo in cui devono essere eseguiti gli aggiornamenti automatici. Per modificare l'intervallo di aggiornamento, è possibile indicare un dato temporale nel campo e modificarlo mediante i tasti freccia a destra del campo.

Ripeti job se il tempo è scaduto

Se l'opzione è attivata, vengono eseguiti job di aggiornamento scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.

11.3.1 Aggiornamento prodotto

In **Aggiornamento prodotto** configurare l'esecuzione degli aggiornamenti del prodotto o la notifica della disponibilità di tali aggiornamenti.

Aggiornamenti prodotto

Scarica aggiornamenti del prodotto e installa automaticamente

Se l'opzione è attivata, gli aggiornamenti del prodotto vengono scaricati e installati automaticamente, non appena si rendono disponibili, dai componenti di aggiornamento. Gli aggiornamenti del file di definizione dei virus e del motore di ricerca avvengono sempre e indipendentemente da questa impostazione. Le premesse per utilizzare questa opzione sono: configurazione completa dell'aggiornamento e collegamento esistente a un server di download.

Scaricare aggiornamenti del prodotto. Se è necessario riavviare, installare l'aggiornamento dopo il successivo riavvio del sistema, altrimenti eseguire immediatamente l'installazione.

Se l'opzione è attivata, gli aggiornamenti del prodotto vengono scaricati non appena disponibili. L'aggiornamento viene installato automaticamente dopo il download dei file di aggiornamento, qualora non sia necessario il riavvio. Se si tratta di un aggiornamento del prodotto che richiede il riavvio del computer, tale aggiornamento non viene eseguito subito dopo il download dei file di aggiornamento, bensì solo dopo il successivo riavvio del sistema effettuato dall'utente. Il vantaggio che ne deriva è che il riavvio non viene eseguito mentre l'utente sta lavorando al computer. Gli aggiornamenti del file di definizione dei virus e del motore di ricerca avvengono sempre e indipendentemente da questa impostazione. Le premesse per utilizzare questa opzione sono: configurazione completa dell'aggiornamento e collegamento esistente a un server di download.

Avvisa quando sono disponibili nuovi aggiornamenti del prodotto

Se l'opzione è attivata, si viene avvisati solo se sono disponibili nuovi aggiornamenti per il prodotto. Gli aggiornamenti del file di definizione dei virus e del motore di ricerca avvengono sempre e indipendentemente da questa impostazione. Le premesse per utilizzare questa opzione sono: configurazione completa dell'aggiornamento e collegamento esistente a un server di download. La notifica avviene tramite un messaggio sul desktop sotto forma di una finestra di pop up e tramite un avviso dell'Updater nel Control Center in Panoramica ::Eventi.

Avvisa nuovamente dopo n giorno(i)

Indicare in questo campo dopo quanti giorni si desidera ricevere nuovamente la notifica relativa alla disponibilità degli aggiornamenti del prodotto, qualora l'aggiornamento del prodotto non sia stato eseguito alla prima notifica.

Non scaricare aggiornamenti prodotto

Se l'opzione è attivata, non si effettuano aggiornamenti automatici o notifiche se sono disponibili aggiornamenti del prodotto mediante l'Updater. Gli aggiornamenti del file di definizione dei virus e del motore di ricerca avvengono sempre e indipendentemente da questa impostazione.

Importante
L'aggiornamento del file di definizione dei virus e del motore di ricerca avviene contestualmente a ogni aggiornamento effettuato, indipendentemente dalle impostazioni di aggiornamento del prodotto (a questo proposito vedere Cap. Aggiornamenti).

11.3.2 Impostazioni riavvio

Quando viene eseguito un aggiornamento del prodotto di AntiVir Personal, può essere necessario un riavvio del sistema. Se è stata impostata un'esecuzione automatica dell'aggiornamento del prodotto in Generale::Aggiornamento::Aggiornamento prodotto, è possibile scegliere fra diverse opzioni di notifica e per l'interruzione del riavvio in **Impostazioni riavvio**.

Nota
Nell'effettuare le impostazioni di riavvio, si noti che nella configurazione è possibile scegliere fra due opzioni per l'esecuzione degli aggiornamenti del prodotto con riavvio necessario del computer, in Generale::Aggiornamento::Aggiornamento prodotto:

Esecuzione automatica dell'aggiornamento del prodotto con riavvio del sistema necessario non appena è disponibile l'aggiornamento: l'aggiornamento e il riavvio vengono eseguiti quando l'utente sta utilizzando il computer. Se è stata attivata questa opzione, possono essere utili le routine di riavvio con possibilità di interruzione oppure con funzione di avviso.

Aggiornamento del prodotto con riavvio del sistema necessario dopo l'avvio successivo: l'aggiornamento e il riavvio vengono eseguiti dopo che l'utente ha avviato il computer e si è registrato. Per questa opzione sono consigliabili le routine di riavvio automatiche.

Impostazioni riavvio

Riavvio del sistema in n secondi

Se l'opzione è attivata, il riavvio necessario viene eseguito **automaticamente** dopo l'esecuzione di un aggiornamento del prodotto secondo l'intervallo di tempo indicato. Compare un conto alla rovescia, senza possibilità di interrompere il riavvio del sistema.

Messaggio di avviso per il riavvio ogni n secondi

Se l'opzione è attivata, il riavvio necessario **non viene eseguito automaticamente** dopo un aggiornamento del prodotto. Nell'intervallo di tempo indicato, vengono visualizzati avvisi di riavvio senza possibilità di interruzione. Negli avvisi è possibile confermare il riavvio del sistema oppure selezionare l'opzione **Ricorda ancora**.

Richiesta di esecuzione di riavvio del sistema

Se l'opzione è attivata, il riavvio necessario **non viene eseguito automaticamente** dopo un aggiornamento del prodotto. Viene visualizzato una sola volta un messaggio in cui è possibile confermare il riavvio oppure interrompere la routine di riavvio.

Riavvio del sistema senza richiesta

Se l'opzione è attivata, il riavvio necessario viene eseguito **automaticamente** dopo un aggiornamento del prodotto. Non si riceve alcun messaggio.

11.3.3 Server web

L'aggiornamento può essere eseguito direttamente mediante server Web in Internet .

Connessione al server Web

Utilizza una connessione esistente (rete)

Questa impostazione viene visualizzata se si utilizza la connessione mediante una rete.

Utilizzare la seguente connessione:

Questa impostazione viene visualizzata se si definisce individualmente la connessione.

L'Updater riconosce automaticamente quali opzioni di connessione sono disponibili. Le opzioni di connessione non disponibili sono grigie e non possono essere attivate. Ad esempio, è possibile creare manualmente una connessione dial-up mediante una voce dell'elenco telefonico di Windows.

- **Utente:** inserire il nome utente dell'account selezionato.
- **Password:** inserire la password per questo account. Per ragioni di sicurezza i caratteri effettivi che si inseriscono in questo campo vengono visualizzati come asterischi (*).

Nota
Se sono stati dimenticati il nome utente o la password di un account Internet contattare il provider di servizi Internet.

Nota
La selezione automatica dell'Updater mediante i cosiddetti tool dial-up (ad esempio SmartSurfer, Oleco, ...) attualmente non è ancora disponibile in Avira AntiVir Personal.

Termina nuovamente la connessione dial-up aperta per l'aggiornamento

Se l'opzione è attivata, la connessione dial-up aperta per l'aggiornamento viene interrotta automaticamente non appena il download è stato eseguito con successo.

Nota
L'opzione non è disponibile in Vista. In Vista la connessione dial-up, aperta per l'aggiornamento, viene sempre interrotta non appena è stato eseguito il download .

11.3.3.1. Proxy

Server proxy

Non utilizzare un server proxy

Se l'opzione è attivata, la connessione al server Web non viene effettuata mediante un server proxy.

Utilizza impostazioni di sistema di Windows

Se l'opzione è attivata, vengono utilizzate le impostazioni di sistema di Windows correnti per la connessione al server Web mediante un server proxy.

Utilizza questo server proxy

Se l'opzione è attivata, la connessione al server Web avviene mediante un server proxy, utilizzando le impostazioni definite dall'utente.

Indirizzo

Immettere l'URL o l'indirizzo IP del server proxy che si desidera utilizzare per la connessione al server Web.

Porta

Inserire il numero della porta del server proxy che si desidera utilizzare per la connessione al server Web.

Nome login

Inserire il proprio nome di login sul server proxy.

Password login

Inserire la password appropriata per la registrazione sul server proxy. Per ragioni di sicurezza i caratteri effettivi che si inseriscono in questo campo vengono visualizzati come asterischi (*).

Esempi:

Indirizzi:	proxy.domain.de	Porta:	8080
Indirizzo:	192.168.1.100	Porta:	3128

11.4 Generale

11.4.1 Configurazione :: Generale

Selezione delle categorie estese delle minacce

Avira AntiVir Personal protegge dai virus del computer.

Inoltre, si ha la possibilità di effettuare una scansione differenziata in base alle seguenti categorie estese delle minacce.

- Software di gestione Backdoor (BDC)
- Programmi di selezione a pagamento (DIALER)
- Giochi (GAMES)
- Programmi ludici (JOKES)
- Security Privacy Risk (SPR)
- Adware/Spyware (ADSPY)
- Programmi zip runtime insoliti (PCK)
- File con estensioni occultate (HEUR-DBLEXT)
- Phishing
- Applicazione (APPL)

Facendo clic sulla casella appropriata viene attivata (spuntata) o disattivata (non spuntata) la modalità selezionata.

Attiva tutti

Se l'opzione è attivata vengono attivate tutte le modalità.

Valori standard

Questo pulsante ripristina i valori standard predefiniti.

Nota
Se viene disattivata una modalità, i file riconosciuti come tale tipo di programma non verranno più segnalati. Non viene riportata alcuna segnalazione nemmeno sul file di report.

11.4.2 Sicurezza

Aggiornamento

Avviso se l'aggiornamento risale a più di n giorni fa

In questo campo è possibile inserire il numero massimo di giorni che possono trascorrere dall'ultimo aggiornamento di Avira AntiVir Personal. Se si supera questo periodo, il Control Center visualizzerà sotto Stato un'icona rossa per lo stato dell'aggiornamento.

Avvisa se il file VDF non è aggiornato

Se l'opzione è attivata, si riceve un avviso in caso di file di definizione dei virus non aggiornato. Grazie all'opzione Avviso, se l'ultimo aggiornamento risale a più di n giorni, è possibile configurare un intervallo temporale.

Tutela del prodotto

Proteggi i processi da una chiusura indesiderata

Se l'opzione è attivata, tutti i processi di AntiVir Personal vengono protetti da chiusura indesiderata dovuta a virus e malware o a una chiusura involontaria di un utente, ad esempio mediante il Task Manager. Questa opzione è attivata di default.

Protezione del processo avanzata

Se l'opzione è attivata, tutti i processi di AntiVir Personal vengono protetti da chiusura indesiderata con metodi avanzati. La protezione avanzata del processo consuma molte più risorse rispetto alla protezione di processo base. Per questo motivo l'opzione è disattivata di default. Per attivare l'opzione è necessario riavviare il computer.

Importante
Protezione del processo in Windows XP 64 Bit non disponibile!

Attenzione
Se la protezione del processo è attivata, possono verificarsi problemi di interazione con altri software. In tal caso disattivare la protezione del processo.

Proteggi i file e le voci di registrazione dalla manipolazione

Se l'opzione è attivata, tutte le voci del registro di AntiVir Personal e tutti i dati del programma (file binari e di configurazione) vengono protetti da manipolazione. La protezione da manipolazione comprende la protezione da interventi di scrittura, eliminazione e talvolta di lettura sulle voci del registro o sui file di programma da parte di utenti o di programmi estranei. Per attivare l'opzione è necessario riavviare il computer.

Nota
Se l'opzione è attivata, è possibile effettuare modifiche della configurazione o di job di scansione e aggiornamento solo tramite l'interfaccia utente.

Importante
Protezione dei file e delle voci di registrazione in Windows XP 64 Bit non disponibile!

11.4.3 WMI

Supporto per Windows Management Instrumentation

Windows Management Instrumentation è una tecnologia di gestione fondamentale di Windows che consente, mediante linguaggi di script e di programmazione in lettura e in scrittura, di accedere in locale e in remoto alle impostazioni dei computer Windows. AntiVir Personal supporta WMI e rende disponibili dati (informazioni di stato, dati statistici, report, job pianificati ecc.), eventi in un'interfaccia. Tramite WMI è possibile richiamare dati operativi di AntiVir Personal .

Attiva supporto WMI

Se l'opzione è attivata, è possibile richiamare i dati operativi di AntiVir Personal tramite WMI.

11.4.4 Directory

Percorso temporaneo

In questo campo inserire il percorso in cui Avira AntiVir Personal salva i propri file temporanei.

Utilizza le impostazioni predefinite

Se l'opzione è attivata vengono utilizzate le impostazioni del sistema per la gestione dei file temporanei.

Nota
I file temporanei nel sistema sono memorizzati ad esempio in Windows XP - in: Start | Impostazioni | Pannello di controllo | Sistema | Scheda "Avanzate" | Pulsanti "Variabili d'ambiente". Le variabili temporanee (TEMP, TMP) per l'utente di volta in volta registrato e per le variabili di sistema (TEMP, TMP) sono visibili qui con i loro rispettivi valori.

Utilizzare la seguente directory

Se l'opzione è attivata viene utilizzato il percorso visualizzato nel campo.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il percorso temporaneo desiderato.

Standard

Il pulsante crea la directory predefinita per il percorso temporaneo.

11.4.5 Eventi

Limitare l'estensione della banca dati degli eventi

Limita l'estensione ad un massimo di n immissioni

Se l'opzione è attiva, il numero massimo delle immissioni nella banca dati degli eventi è limitato a un preciso numero; i valori consentiti sono: da 100 a 10.000 immissioni. Se il numero delle immissioni viene superato gli inserimenti più vecchi vengono eliminati.

Elimina tutti gli eventi più vecchi di n giorno/i

Se l'opzione è attiva dopo un numero determinato di giorni gli eventi vengono eliminati dalla banca dati degli eventi; i valori consentiti sono: da 1 a 90 giorni. Di default questa opzione è attivata con un valore di 30 giorni.

Non limitare estensione banca dati (elimina eventi manualmente)

Con l'opzione attivata, le dimensioni della banca dati degli eventi non sono limitate. Sull'interfaccia del programma, alla voce Eventi, viene però visualizzato un massimo di 20.000 immissioni.

11.4.6 Limita i report

Limita il numero di report

Limita il numero a n pezzi

Se l'opzione è attiva, il numero massimo di report può essere limitato; i valori consentiti sono: da 1 a 300. Se il numero indicato viene superato, i report più vecchi vengono eliminati.

Elimina tutti i report più vecchi di n giorni

Se l'opzione è attiva i report vengono automaticamente eliminati dopo un determinato numero di giorni; i valori consentiti sono: da 1 a 90 giorni. Di default questa opzione è attivata con un valore di 30 giorni.

Non limitare il numero dei report (elimina manualmente i report)

Se l'opzione è attiva il numero di report non è limitato.

11.4.7 Avvisi acustici

Avviso acustico

In caso di rilevamento di un virus o di un malware tramite sistema di scansione o Guard viene emesso un avviso acustico in modalità di azione interattiva. È possibile attivare o disattivare l'avviso acustico oppure selezionare un file wave alternativo come avviso acustico.

Nota
La modalità di azione del sistema di scansione viene impostata nella configurazione in Sistema di scansione::Scansione::Azione in caso di rilevamento.

Nessun avviso

Se l'opzione è attivata, non viene emesso alcun avviso acustico in caso di rilevamento tramite il sistema di scansione o il Guard.

Emetti tramite casse PC (solo in modalità interattiva)

Se l'opzione è attivata, viene emesso un avviso acustico con suono standard in caso di rilevamento di un virus tramite sistema di scansione o Guard. L'avviso acustico viene emesso tramite l'altoparlante interno del PC.

Utilizza il seguente file wave (solo in modalità interattiva)

Se l'opzione è attivata, in caso di rilevamento di un virus tramite sistema di scansione o Guard viene emesso un avviso acustico con il file wave selezionato. Il file wave selezionato viene riprodotto tramite un altoparlante collegato esternamente.

File audio (.WAV)

In questo campo è possibile inserire il nome e il percorso corrispondente di un file audio. L'avviso acustico standard di AntiVir Personal viene immesso di default.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il file desiderato grazie all'explorer dei file.

Test

Questo pulsante serve a testare il file wave selezionato.

11.4.8 Avvisi

In caso di determinati eventi, AntiVir Personal genera notifiche sul desktop, i cosiddetti messaggi a tendina, per informare l'utente di eventuali pericoli o della riuscita o meno dell'esecuzione di un dato programma come, per esempio, un aggiornamento. È possibile attivare o disattivare in *Avvisi* la funzione di notifica per specifici eventi.

Nel caso delle notifiche sul desktop è possibile disattivare direttamente le notifiche sul messaggio a tendina. È possibile annullare la disattivazione della notifica in *Avvisi*.

Avvisi

sulle connessioni dial-up utilizzate

Se l'opzione è attivata, l'utente è avvisato con una notifica sul desktop quando un programma di selezione stabilisce una connessione sul computer tramite la rete telefonica o ISDN. In caso di programmi di selezione esiste il rischio che si tratti di un dialer sconosciuto e indesiderato, che stabilisce una connessione a pagamento. (vedere Virus e altro::Categorie estese delle minacce: Dialer).

sul corretto aggiornamento dei file

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando è stato completato con successo un aggiornamento e sono stati aggiornati file.

su aggiornamento fallito

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando un aggiornamento non è stato completato con successo: Non è stato possibile stabilire una connessione con il server di download o non è stato possibile installare i file aggiornati.

non è necessario alcun aggiornamento

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando è stato lanciato un aggiornamento ma non era necessario installare alcun file perché il programma era già aggiornato.

registrazione con i diritti di amministratore

Se l'opzione è attivata, dopo la registrazione sul computer, l'utente riceve un avviso se il suo account utente prevede anche diritti di amministratore. Per motivi di sicurezza si consiglia generalmente di lavorare con un account utente limitato. Lavorando sul computer con diritti utente limitati, l'utente previene l'installazione automatica di programmi indesiderati e la modifica involontaria delle impostazioni di sistema.

Avira AntiVir Personal – Free Antivirus

www.avira.it

Achab S.r.l.

Piazza Cinque Giornate, 4
20129 Milano
Italia
Telefono: +39.02.54108204
Fax: +39.02.5461894
Internet: http://www.avira.it

AntiVir® è un marchio registrato di Avira GmbH. Tutti gli altri marchi o nomi di prodotti sono marchi registrati del legittimo proprietario. I marchi protetti non sono contrassegnati come tali in questo manuale. Ciò tuttavia non significa che possano essere liberamente utilizzati.

© 2010 Avira GmbH.
Tutti i diritti riservati.

Il presente manuale è stato redatto con la massima cura, tuttavia non si può escludere la presenza di errori nella forma o nel contenuto. Non è permesso alcun tipo di riproduzione della presente pubblicazione o di parti di essa senza il previo consenso scritto di Avira GmbH.

Salvo errori e modifiche tecniche.

AVIRA®